

Vigor2710-Serie
ADSL2/2+ Firewall-Router
Benutzerhandbuch

Version: 1.1

Datum: 15.07.2009

Hinweise zum Urheberrecht

Warenzeichen

Die folgenden Warenzeichen werden in diesem Dokument verwendet:

- Microsoft ist ein eingetragenes Warenzeichen der Microsoft Corp.
- Windows, Windows 95, 98, Me, NT, 2000, XP, Vista und Explorer sind Warenzeichen der Microsoft Corp.
- Apple und Mac OS sind eingetragene Warenzeichen von Apple Inc.
- Andere Produkte können Warenzeichen oder eingetragene Warenzeichen der entsprechenden Hersteller sein.

Sicherheitshinweise und Genehmigung

Sicherheitshinweise

- Lesen Sie die Installationsanweisungen sorgfältig durch, bevor Sie den Router einrichten.
- Der Router ist ein kompliziertes elektronisches Gerät, das nur durch autorisiertes, qualifiziertes Personal repariert werden darf. Versuchen Sie nicht, den Router selbst zu öffnen oder zu reparieren.
- Stellen Sie den Router nicht an einem feuchten Ort auf (z.B. Badezimmer).
- Der Router sollte an einem geschützten Ort in einem Temperaturbereich von +5 bis +40°C betrieben werden.
- Setzen Sie den Router nicht direktem Sonnenlicht oder anderen Wärmequellen aus. Das Gehäuse und elektronische Bauteile können durch direktes Sonnenlicht oder Wärmequellen geschädigt werden.
- Um Gefahren durch elektronische Schläge zu vermeiden, setzen Sie das LAN-Verbindungskabel nicht im Außenbereich ein.
- Halten Sie die Verpackung von Kindern fern.
- Bei der Entsorgung des Routers bitte örtliche Naturschutzvorschriften beachten.

Gewährleistung

Wir garantieren dem ursprünglichen Endbenutzer (Käufer), dass der Router für einen Zeitraum von zwei (2) Jahren ab Kaufdatum frei von Herstellungs- und Werkstofffehlern sein wird. Bitte bewahren Sie Ihren Kaufbeleg gut auf, da dieser als Nachweis des Kaufdatums dient. Sollte das Produkt während des Gewährleistungszeitraums Mängel aufweisen, die auf fehlerhafter Herstellung und/oder Werkstoffen beruhen, werden wir gegen Vorlage des Kaufbelegs nach eigenem Ermessen die mangelhaften Produkte oder Bauteile ohne Berechnung von Ersatzteil- und Arbeitszeitkosten so reparieren oder ersetzen, wie wir es für notwendig erachten, um das Produkt in den einwandfreien Betriebszustand zu versetzen. Bei ersetzten Produkten handelt es sich um neue oder überarbeitete, funktional gleichwertige Produkte, die wir nach eigenem Ermessen anbieten. Die Gewährleistung gilt nicht, wenn das Produkt modifiziert, missbraucht, manipuliert, durch höhere Gewalt geschädigt oder anormalen Betriebsbedingungen ausgesetzt wird. Die Gewährleistung umfasst nicht die gebündelte oder lizenzierte Software anderer Hersteller. Mängel, welche die Gebrauchsfähigkeit des Produkts nicht wesentlich einschränken, werden durch die Gewährleistung nicht abgedeckt. Wir behalten uns vor, das Handbuch und die Online-Dokumentation zu revidieren und die Inhalte gegebenenfalls zu ändern, ohne dass wir verpflichtet wären, irgendeine Person über solche Revisionen oder Änderungen zu benachrichtigen.

Werden Sie ein registrierter Benutzer

Online-Registrierung wird empfohlen. Sie können Ihren Vigor-Router unter http://www.draytek.de registrieren.

Firmware- und Tool-Aktualisierungen

Aufgrund der ständigen Weiterentwicklung der DrayTek-Technologie werden die Router regelmäßig verbessert. Weitere Informationen zur neuesten Firmware, Tools und Dokumenten werden auf der DrayTek Web-Site vorgehalten.

http://www.draytek.de

EG-Erklärungen

Hersteller: DrayTek Corp.
Adresse: No. 26, Fu Shing Road, HuKou County, HsinChu Industrial Park, Hsin-Chu, Taiwan 303

Produkt: Router der Vigor2710-Serie

DrayTek Corp. erklärt hiermit, dass die Router der Vigor2820-Serie den folgenden wesentlichen Anforderungen und anderen relevanten Bestimmungen der R&TTE-Richtlinie 1999/5/EG entsprechen.

Das Produkt entspricht durch Erfüllung der Anforderungen von EN55022/Klasse B und EN55024/Klasse B den Anforderungen der EMV-Richtlinie 2004/108/EG.

Das Produkt entspricht durch Erfüllung der Anforderungen von EN60950-1 den Anforderungen der Niederspannungsrichtlinie 2006/95/EG.

Aufsichtsrechtlicher Hinweis

FCC-Erklärung

Dieses Gerät wurde getestet und entspricht den Grenzwerten für digitale Geräte der Klasse B gemäß Teil 15 der FCC-Richtlinien. Diese Grenzwerte wurden definiert, um einen angemessenen Schutz gegen Funkstörungen in häuslichen Umgebungen sicherzustellen. Dieses Gerät kann Radiofrequenzenergie generieren, verwenden und ausstrahlen. Wird das Gerät nicht gemäß den Anweisungen installiert und verwendet, kann es zu Überlagerungen bei Funkübertragungen kommen. Es kann nicht garantiert werden, dass Funkstörungen bei einer bestimmten Installation nicht auftreten. Sollte dieses Gerät den Radio- oder Fernsehempfang stören, was festgestellt werden kann, indem das Gerät aus- und wieder eingeschaltet wird, ist der Benutzer angehalten, die Funkstörung durch eine der folgenden Maßnahmen zu beseitigen:

- Ausrichtung oder Standort der Empfangsantenne ändern.
- Entfernung zwischen dem Gerät und dem Empfänger vergrößern.
- Verbinden Sie das Gerät und den Empfänger mit getrennten Steckdosen bzw. Stromkreisen.
- Wenden Sie sich an den Fachhändler oder an einen erfahrenen Radio-/Fernsehtechniker.

Dieses Gerät entspricht Teil 15 der FCC-Richtlinien. Der Betrieb ist unter den folgenden zwei Bedingungen gestattet:

(1) Dieses Gerät darf keine Störungen verursachen.

(2) Dieses Gerät muss alle empfangenen Störungen , einschließlich Störungen, die einen unerwünschten Betrieb zur Folge haben, akzeptieren.

Bitte besuchen Sie http://www.draytek.com/about_us/R_TTE_Certification.php.



Dieses Produkt ist für DSL-, POTS- und 2,4-GHz-WLAN-Netzwerke in der gesamten EU und in der Schweiz sowie mit Einschränkungen in Frankreich geeignet. Die verfügbaren Netzwerke sind auf Ihrem Produkt angegeben.

Inhaltsverzeichnis

Vorwort..1

1.1 Erläuterung der Web-Konfigurationstasten....................................1

1.2 LED-Anzeigen und Anschlüsse....................................2

1.2.1 Vigor2710....................................2
1.2.2 Vigor2710n....................................4
1.2.3 Vigor2710Vn....................................6

1.3 Hardwareinstallation....................................8

1.4 Druckerinstallation....................................9

Grundlegende Einstellungen....................................14

2.1 Zweistufiges Management....................................14

2.2 Zugriff auf die Web-Seite....................................14

2.3 Passwort ändern....................................15

2.4 Schnellstart-Assistent....................................17

2.4.1 Auswahl Protokoll/Kapselung....................................17
2.4.2 PPPoE/PPPoA....................................18
2.4.3 1483 Bridged IP....................................20
2.4.4 1483 Routed IP....................................20

2.5 Onlinestatus....................................21

2.6 Konfiguration speichern....................................23

Benutzermodus....................................24

3.1 Einwahl ins Internet....................................24

3.1.1 Grundlagen des Internet Protocol (IP) Netzwerks....................................24
3.1.2 PPPoE/PPPoA....................................25

3.2 LAN....................................31

3.2.1 LAN-Grundlagen....................................31
3.2.2 Basiskonfiguration....................................32

3.3 NAT....................................36

3.3.1 Portumleitung....................................36
3.3.2 DMZ-Host....................................39
3.3.3 Offene Ports....................................41

3.4 Anwendungen....................................43

3.4.1 Dynamisches DNS....................................43
3.4.2 UPnP....................................45

3.5 Wireless LAN....................................48

3.5.1 Grundlagen....................................48
3.5.2Basiskonfiguration....................................50
3.5.3 Verschlüsselung....................................53
3.5.4 Zugriffskontrolle....................................54
3.5.5 Liste der Clients....................................55

3.6 Systemmanagement....................................56

3.6.1 Systemstatus....................................56
3.6.2 Benutzerpasswort....................................57
3.6.3 Zeit und Datum....................................57

3.6.4 Neustart.....58
3.7 Diagnose-Tools.....59
3.7.1 DHCP-Tabelle.....59
3.7.2 Ping.....60
3.7.3 Trace Route.....61
Administratormodus.....62
4.1 Einwahl ins Internet.....62
4.1.1 Grundlagen des Internet Protocol (IP) Netzwerks.....62
4.1.2 PPPoE/PPPoA.....63
4.1.3 Multi-PVCs.....69
4.2 LAN.....73
4.2.1 LAN-Grundlagen.....73
4.2.2 Basiskonfiguration.....75
4.2.3 Feste Adressumleitung.....78
4.2.4 VLAN.....82
4.2.5 IP an MAC binden.....83
4.3 NAT.....85
4.3.1 Portumleitung.....85
4.3.2 DMZ-Host.....88
4.3.3 Offene Ports.....90
4.4 Firewall.....92
4.4.1 Firewall-Grundlagen.....92
4.4.2 Basiskonfiguration.....94
4.4.3 Filtereinstellung.....96
4.4.4 DoS-Abwehr.....101
4.5 Objekte.....104
4.5.1 IP-Objekt.....104
4.5.2 IP-Gruppe.....106
4.5.3 Servicetyp-Objekt.....107
4.5.4 Servicetyp-Gruppe.....109
4.5.5 Stichwort-Objekt.....110
4.5.6 Stichwort-Gruppe.....111
4.5.7 Dateiformat-Objekt.....112
.....113
4.5.8 IM-Objekt.....114
4.5.9 P2P-Objekt.....115
4.5.10 Diverses.....116
4.6 CSM-Profil.....117
4.6.1 IM-/P2P-Filter.....118
4.6.2 Inhaltsbezogener URL-Filter.....119
4.6.3 Inhaltsbezogener Web-Filter.....123
4.7 Bandbreitenmanagement.....125
4.7.1 Sitzungen begrenzen.....125
4.7.2 Bandbreitenbegrenzung.....127
4.7.3 QoS.....128
4.8 Anwendungen.....135
4.8.1 Dynamisches DNS.....135
4.8.2 Verbindungstimer.....137
4.8.3 RADIUS.....140
4.8.4 UPnP.....141

4.8.5 IGMP....143
4.8.6 Wake on LAN....144

4.9 VPN und externe Einwahl....145

4.9.1 Einwahlmöglichkeiten....145
4.9.2 PPP-Einstellungen....146
4.9.3 IPSec Grundeinstellungen....147
4.9.4 IPSec-Identität....149
4.9.5 Externe Benutzer....151
4.9.6 LAN zu LAN....154
4.9.7 Verbindungsmanagement....161

4.10 Zertifikatsverwaltung....162

4.10.1 Lokales Zertifikat....162
4.10.2 Vertrauenswürdiges CA-Zertifikat....164
4.10.3 Zertifikat sichern....165

4.11 Wireless LAN....166

4.11.1 Grundlagen....166
4.11.2 Basiskonfiguration....168
4.11.3 Verschlüsselung....171
4.11.4 Zugriffskontrolle....173
4.11.5 WPS....174
4.11.6 WDS....176
4.11.7 Liste der Access Points....179
4.11.8 Liste der Clients....181

4.12 Systemmanagement....182

4.12.1 Systemstatus....182
4.12.2 TR-069....183
4.12.3 Administratorpasswort....184
4.12.4 Sicherung der Konfiguration....184
4.12.5 Syslog/Mail-Alarm....186
4.12.6 Zeit und Datum....188
4.12.7 Verwaltung....189
4.12.8 Neustart....190
4.12.9 Firmware aktualisieren....191

4.13 Diagnose-Tools....192

4.13.1 Anwahlauslöser....192
4.13.2 Routing-Tabelle....193
4.13.3 ARP-Cache-Tabelle....193
4.13.4 DHCP-Tabelle....194
4.13.5 NAT-Sitzungstabelle....194
4.13.6 Datenfluss-Monitor....195
4.13.7 Traffic-Diagramm....196
4.13.8 Ping....197
4.13.9 Trace Route....198

Anwendung und Beispiele....199

5.1 LAN-zu-LAN-Verbindung zwischen Filiale und Zentrale einrichten....199

5.2 Einwahlverbindung zwischen externem Teleworker und Zentrale einrichten....206

5.3 Beispiel für QoS-Einstellungen....211

5.4 LAN – Einrichtung mit NAT....215

5.5 Firmware des Routers aktualisieren....217

5.6 Zertifikat von einem CA-Server oder Windows CA-Server anfordern....218

5.7 CA-Zertifikat von Windows CA-Server anfordern und als vertrauenswürdiges Zertifikat setzen....222

Fehlersuche....224

6.1 Hardwarestatus überprüfen....224

6.2 Netzwerkeinstellungen am PC kontrollieren....225

6.3 Pingen des Routers von Ihrem PC aus....227

6.4 Prüfen der ISP-Einstellungen....228

6.5 Auf Werkseinstellungen zurücksetzen (Factory-Reset)....229

6.6 Technische Hilfe....230

1 Vorwort

Bei der Vigor2710-Serie handelt es sich um einen ADSL-Router. Der Router bietet QoS auf IP-Ebene sowie NAT Sitzungs-/Bandbreitenmanagement, um bei großen Bandbreiten effektive Benutzerkontrolle zu ermöglichen.

Durch den Einsatz der hardwarebasierten VPN-Plattform und AES/DES/3DS-Hardwareverschlüsselung steigert der Router die VPN-Leistung enorm und bietet verschiedene Protokolle (wie IPSec/PPTP/L2TP) mit bis zu zwei VPN-Tunneln.

Das objektbasierte Konzept, das in der SPI-Firewall (Stateful Packet Inspection) verwendet wird, erleichtert Benutzern die Einrichtung der Firewall-Regeln. CSM (Content Security Management) gibt Benutzern effizientere Kontrolle im Umgang mit IM (Instant Messenger) und P2P (Peer to Peer). DoS/DDoS-Schutz und inhaltsbezogene URL-/Web-Filter verbessern die externe Sicherheit und die interne Kontrolle.

Die objektbasierte Firewall ist flexibel und macht Ihr Netzwerk sicher. Durch die VoIP-Funktion können Sie und Ihre Gesprächspartner Kommunikationskosten sparen.

Außerdem verfügt die Vigor2710-Serie über eine USB-Schnittstelle, an die USB-Drucker als Netzwerkdrucker oder USB-Speichergeräte für gemeinsamen Dateizugriff angeschlossen werden können. Die Vigor2710-Serie bietet ein zweistufiges Management, um die Konfiguration der Netzwerkverbindung zu vereinfachen. Der Benutzermodus ermöglicht Benutzern Zugriff auf die Web-Oberfläche zur einfachen Konfiguration. Benutzer, die erweiterte Konfigurationsmöglichkeiten wünschen, können die Web-Oberfläche im Administratormodus nutzen.

1.1 Erläuterung der Web-Konfigurationstasten

In der Web-Oberfläche werden die folgenden Schaltflächen häufig verwendet:

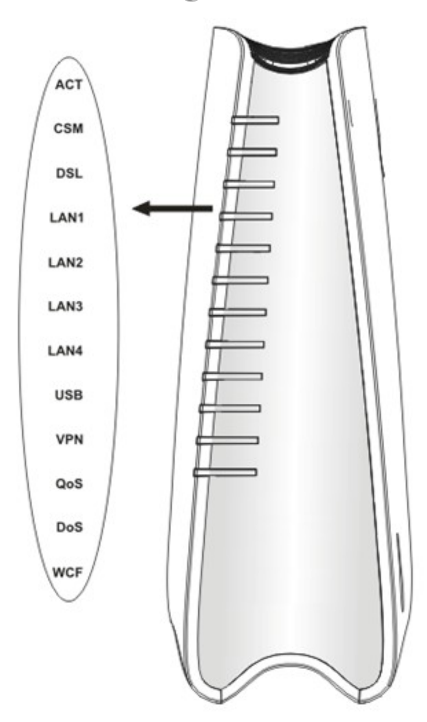
OK	Speichern und aktuelle Einstellungen anwenden.
Abbrechen	Aktuelle Einstellungen abbrechen und vorher gespeicherte Einstellungen wiederherstellen.
Hinzufügen	Neue Einstellungen für den jeweiligen Punkt hinzufügen.
Bearbeiten	Einstellungen des ausgewählten Punktes bearbeiten.
Löschen	Ausgewählten Punkt mit den entsprechenden Einstellungen löschen.

Hinweis: Die anderen in der Web-Oberfläche angezeigten Schaltflächen werden in Kapitel 4 detailliert erläutert.

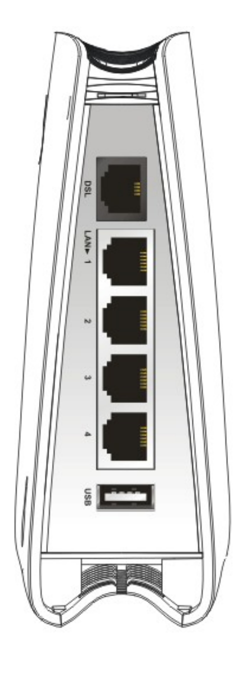
1.2 LED-Anzeigen und Anschlüsse

Bevor Sie den Vigor-Router verwenden, machen Sie sich bitte mit den LED-Anzeigen und Anschlüssen vertraut.

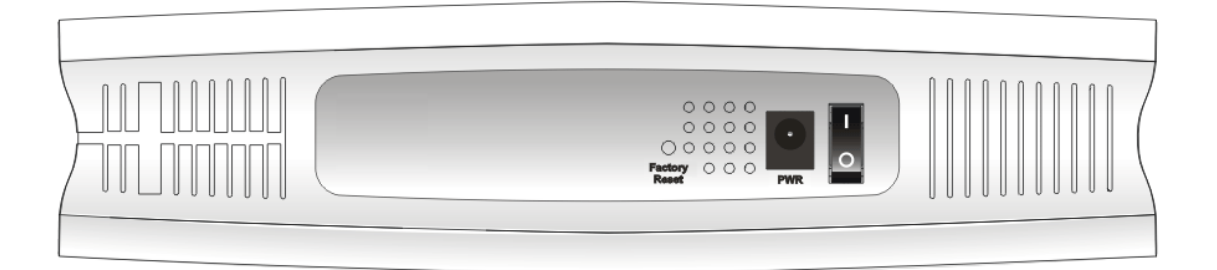
1.2.1 Vigor2710



LED	Status	Erläuterung
ACT (Aktivität)	Blinkt	Der Router ist eingeschaltet und funktioniert ordnungsgemäß.
	Aus	Der Router ist ausgeschaltet.
CSM	Ein	Das/die CSM-Profil(e) (Content Security Management) für den IM/P2P, inhaltsbezogene URL-/Web-Filter kann/können unter **Firewall >>Basiskonfiguration** aktiviert werden. (Das eigentliche Profil muss im **CSM**-Menü eingerichtet werden.)
DSL	Ein	Der Router ist bereit für den Zugriff auf das Internet über den DSL-Link.
	Blinkt	Langsam: Das Modem ist bereit. Schnell: Die Verbindung wird angepasst.
LAN 1/2/3/4	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
USB	Ein	Ein USB-Gerät ist angeschlossen und aktiv.
	Blinkt	Es werden Daten übertragen.
VPN	Ein	Der VPN-Tunnel ist aktiv.
QoS	Ein	Die QoS-Funktion ist aktiv.
DoS	Ein	Die DoS/DDoS-Funktion ist aktiv.
	Blinkt	Blinkt bei Erkennung eines Angriffs.
WCF	Ein	Das/die CSM-Profil(e) (Content Security Management) für den inhaltsbezogenen Web-Filter kann/können unter **Firewall >>Basiskonfiguration** aktiviert werden. (Das eigentliche Profil muss im **CSM**-Menü eingerichtet werden.)

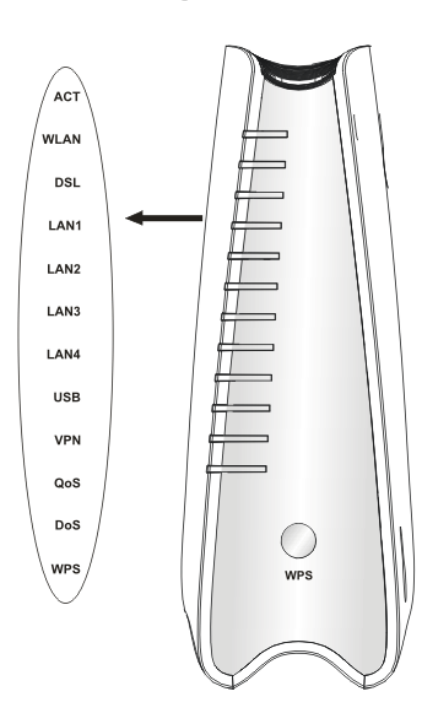


Schnittstelle	Beschreibung
DSL	Anschluss für Zugriff auf das Internet per ADSL2/2+
LAN (1-4)	Anschlüsse für lokale Netzwerkgeräte
USB	Anschluss für USB-Speichermedium (USB-Stick, USB-Festplatte) oder Drucker

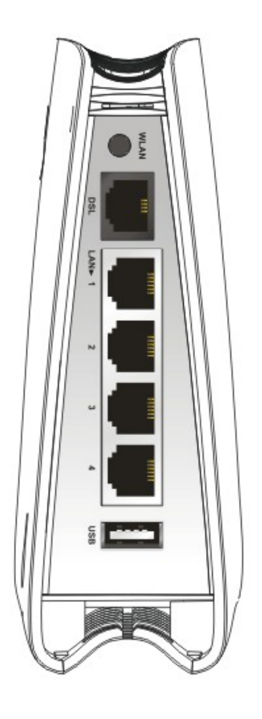


Schnittstelle	Beschreibung
Factory Reset	Standardeinstellungen wiederherstellen. Verwendung: Schalten Sie den Router ein (ACT LED blinkt). Halten Sie den eingelassenen Knopf mindestens fünf Sekunden lang gedrückt. Sobald die ACT LED schneller als sonst zu blinken beginnt, lassen Sie den Knopf los. Der Router wird daraufhin mit den Werkseinstellungen neu gestartet.
PWR	Anschluss für das Netzteil
EIN/AUS	Netzschalter

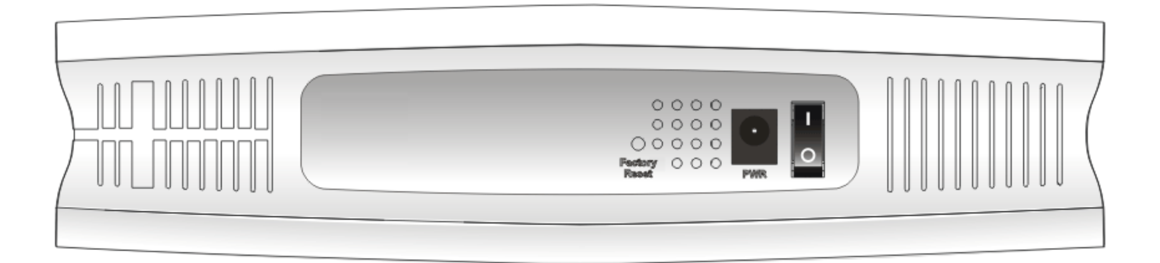
1.2.2 Vigor2710n



LED	Status	Erläuterung
ACT (Aktivität)	Blinkt	Der Router ist eingeschaltet und funktioniert ordnungsgemäß.
	Aus	Der Router ist ausgeschaltet.
WLAN	Ein	Der Wireless Access Point ist bereit.
	Blinkt	Wireless-Datenverkehr
DSL	Ein	Der Router ist bereit für den Zugriff auf das Internet über den DSL-Link.
	Blinkt	Langsam: Das Modem ist bereit. Schnell: Die Verbindung wird angepasst.
LAN 1/2/3/4	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
USB	Ein	Ein USB-Gerät ist angeschlossen und aktiv.
	Blinkt	Es werden Daten übertragen.
VPN	Ein	Der VPN-Tunnel ist aktiv.
QoS	Ein	Die QoS-Funktion ist aktiv.
DoS	Ein	Die DoS/DDoS-Funktion ist aktiv.
	Blinkt	Blinkt bei Erkennung eines Angriffs.
WPS	Ein	WPS ist eingeschaltet.
	Aus	WPS ist ausgeschaltet.
	Blinkt	Wartet ca. zwei Minuten auf Verbindungsanforderungen von Wireless-Clients.
WPS-Knopf	Ein	Halten Sie diesen Knopf zwei Sekunden lang gedrückt, um auf den Aufbau einer WPS-Netzwerkverbindung des Client-Geräts zu warten. Wenn die LED aufleuchtet, ist WPS aktiv.
	Aus	WPS ist ausgeschaltet.
	Blinkt	Wartet ca. zwei Minuten auf Verbindungsanforderungen von Wireless-Clients.

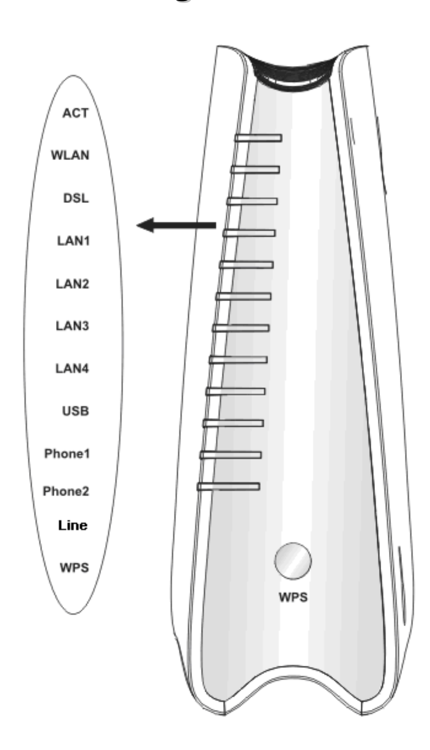


Schnittstelle	Beschreibung
WLAN	Drücken Sie den Knopf einmal, um die Wireless-Verbindung zu aktivieren (WLAN LED ein) oder zu deaktivieren (WLAN LED aus).
DSL	Anschluss für Zugriff auf das Internet per ADSL2/2+
LAN (1-4)	Anschlüsse für lokale Netzwerkgeräte
USB	Anschluss für USB-Speichermedium (USB-Stick, USB-Festplatte) oder Drucker

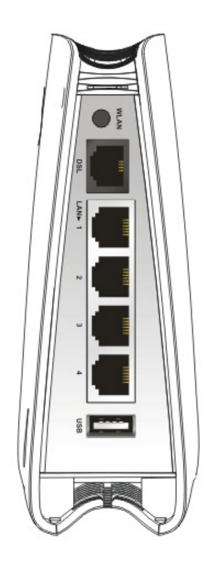


Schnittstelle	Beschreibung
Factory Reset	Standardeinstellungen wiederherstellen. Verwendung: Schalten Sie den Router ein (ACT LED blinkt). Halten Sie den eingelassenen Knopf mindestens fünf Sekunden lang gedrückt. Sobald die ACT LED schneller als sonst zu blinken beginnt, lassen Sie den Knopf los. Der Router wird daraufhin mit den Werkseinstellungen neu gestartet.
PWR	Anschluss für das Netzteil
EIN/AUS	Netzschalter

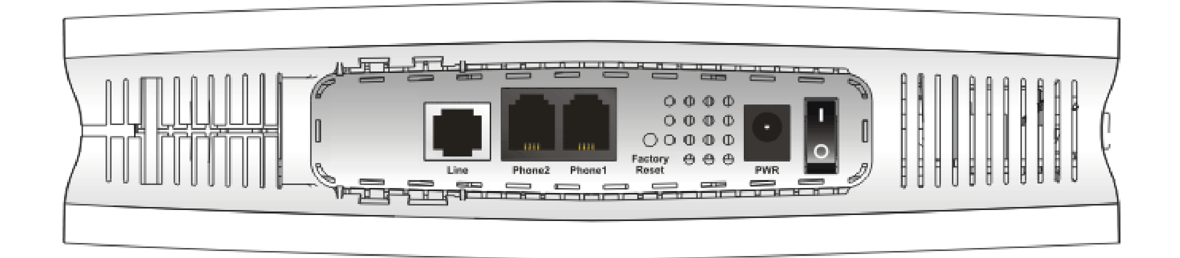
1.2.3 Vigor2710Vn



LED	Status	Erläuterung
ACT (Aktivität)	Blinkt	Der Router ist eingeschaltet und funktioniert ordnungsgemäß.
	Aus	Der Router ist ausgeschaltet.
WLAN	Ein	Der Wireless Access Point ist bereit.
	Blinkt	Wireless-Datenverkehr
DSL	Ein	Der Router ist bereit für den Zugriff auf das Internet über den DSL-Link.
	Blinkt	Langsam: Das Modem ist bereit. Schnell: Die Verbindung wird angepasst.
LAN 1/2/3/4	Ein	Der Port ist verbunden.
	Aus	Der Port ist nicht verbunden.
	Blinkt	Es werden Daten übertragen.
USB	Ein	Ein USB-Gerät ist angeschlossen und aktiv.
	Blinkt	Es werden Daten übertragen.
Phone1/ Phone2	Ein	Das an diesem Port angeschlossene Telefon wurde abgenommen.
	Aus	Das an diesem Port angeschlossene Telefon ist aufgelegt.
	Blinkt	Eingehender Anruf
Line	Ein	Ein- oder ausgehender PSTN-Anruf. Wenn der Anruf beendet wird, erlischt die LED nach ca. sechs Sekunden.
	Aus	Kein PSTN-Telefonanruf
WPS	Ein	WPS ist eingeschaltet.
	Aus	WPS ist ausgeschaltet.
	Blinkt	Wartet ca. zwei Minuten auf Verbindungsanforderungen von Wireless-Clients.
WPS-Knopf	Ein	Halten Sie diesen Knopf zwei Sekunden lang gedrückt, um auf den Aufbau einer WPS-Netzwerkverbindung des Client-Geräts zu warten. Wenn die LED aufleuchtet, ist WPS aktiv.
	Aus	WPS ist ausgeschaltet.
	Blinkt	Wartet ca. zwei Minuten auf Verbindungsanforderungen von Wireless-Clients.



Schnittstelle	Beschreibung
WLAN	Drücken Sie den Knopf einmal, um die Wireless-Verbindung zu aktivieren (WLAN LED ein) oder zu deaktivieren (WLAN LED aus).
DSL	Anschluss für Zugriff auf das Internet per ADSL2/2+
LAN (1-4)	Anschlüsse für lokale Netzwerkgeräte
USB	Anschluss für USB-Speichermedium (USB-Stick, USB-Festplatte) oder Drucker

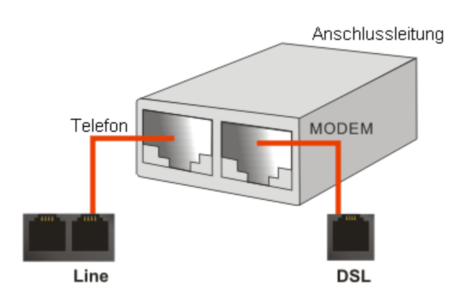


Schnittstelle	Beschreibung
Line	PSTN-Anschluss für analoges Telefon
Phone2/Phone1	Anschluss für analoges Telefon für VoIP-Kommunikation
Factory Reset	Standardeinstellungen wiederherstellen. Verwendung: Schalten Sie den Router ein (ACT LED blinkt). Halten Sie den eingelassenen Knopf mindestens fünf Sekunden lang gedrückt. Sobald die ACT LED schneller als sonst zu blinken beginnt, lassen Sie den Knopf los. Der Router wird daraufhin mit den Werkseinstellungen neu gestartet.
PWR	Anschluss für das Netzteil
EIN/AUS	Netzschalter

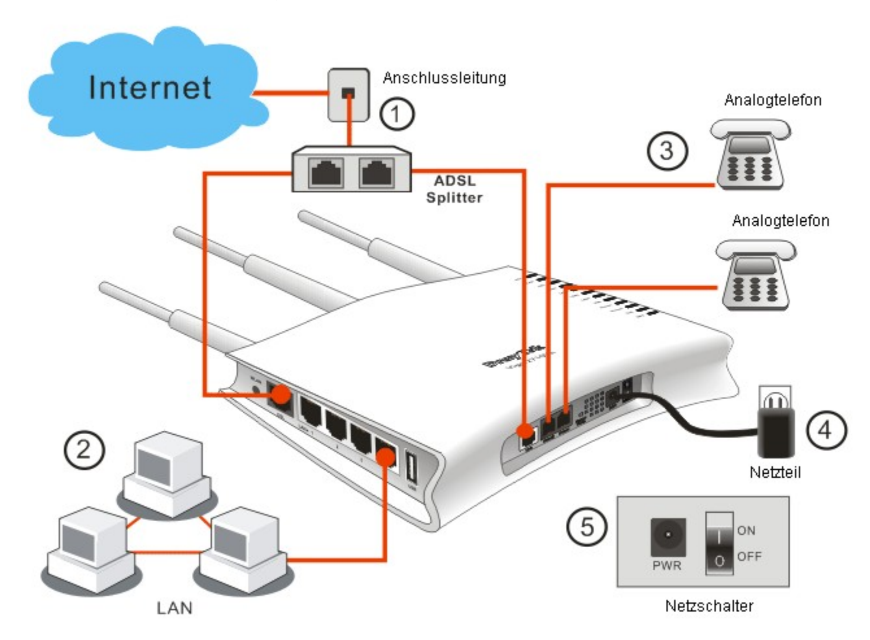
1.3 Hardwareinstallation

Bevor Sie den Router konfigurieren, müssen Sie Ihre Geräte ordnungsgemäß anschließen.

1. Verbinden Sie bei allen Modellen die ADSL-Schnittstelle mit Hilfe des ADSL-Kabels mit dem externen ADSL-Splitter. Beim Vigor2710Vn verbinden Sie auch die Line-Schnittstelle mit dem externen ADSL-Splitter.



2. Verbinden Sie ein Ende eines Ethernet-Kabels (RJ-45) mit einem der **LAN**-Ports am Router und das andere Ende des Kabels (RJ-45) mit dem Ethernet-Port Ihres Rechners.
3. Verbinden Sie den Telefonapparat mit Hilfe eines Telefonkabels (um die VoIP-Funktion zu verwenden). Beim Modell ohne Telefonanschluss überspringen Sie diesen Schritt.
4. Verbinden den Ausgang des Netzteils mit dem Netzanschluss auf der Rückseite und das andere Ende mit einer Steckdose.
5. Schalten Sie das Gerät ein, indem Sie auf den Netzschalter auf der Rückseite drücken.
6. Das System wird initialisiert. Nach Abschluss des Systemtests leuchtet die **ACT** LED auf und fängt an, zu blinken.

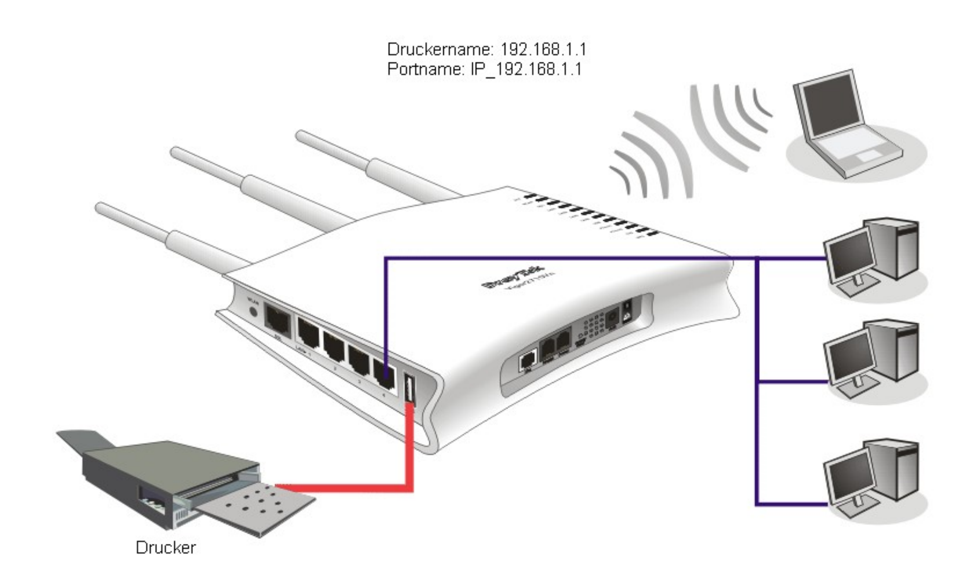


(Einzelheiten zum LED-Status werden in Abschnitt 1.2 erläutert.)

Achtung: Jeder Telefonanschluss darf nur mit einem analogen Telefon verbunden werden. Verbinden Sie die Telefonanschlüsse nicht mit der Telefonsteckdose. Eine solche Verbindung kann Ihren Router beschädigen.

1.4 Druckerinstallation

Sie können mit dem Router einen Netzwerkdrucker installieren. Alle an diesem Router angeschlossenen Rechner können über den Router drucken. Das hier gezeigte Beispiel verwendet Windows XP/2000. Für Windows 98/SE/Vista kontaktieren Sie bitte **support@draytek.de**.



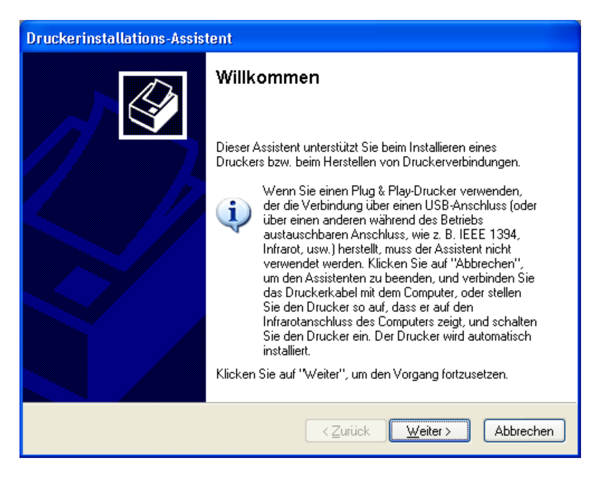
Bevor Sie den Drucker verwenden, konfigurieren Sie die angeschlossenen Rechner (oder Wireless-Clients) bitte wie folgt.

1. Verbinden Sie den Drucker über die USB-/parallele Schnittstelle mit dem Router.
2. Öffnen Sie **Start->Systemsteuerung-> Drucker und Faxgeräte**.

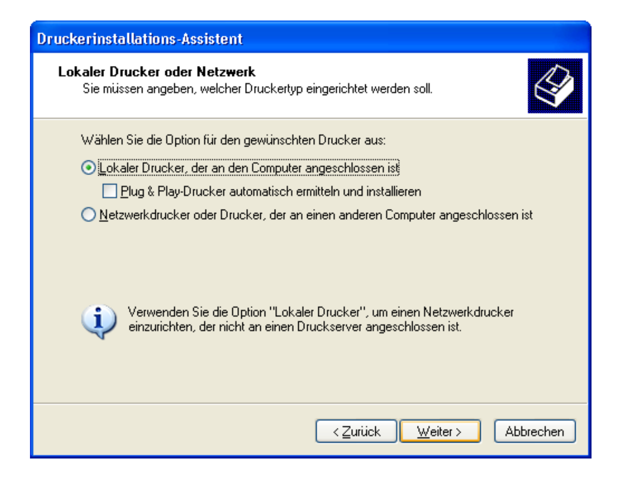


3. Öffnen Sie **Datei->Drucker hinzufügen**. Der Druckerinstallations-Assistent erscheint. Klicken Sie auf **Weiter**.

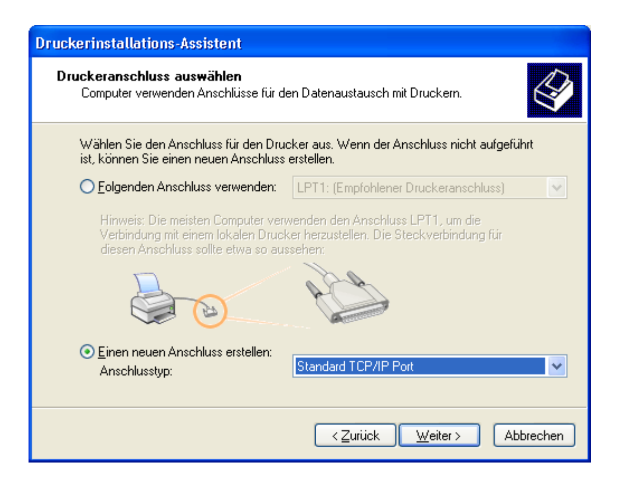




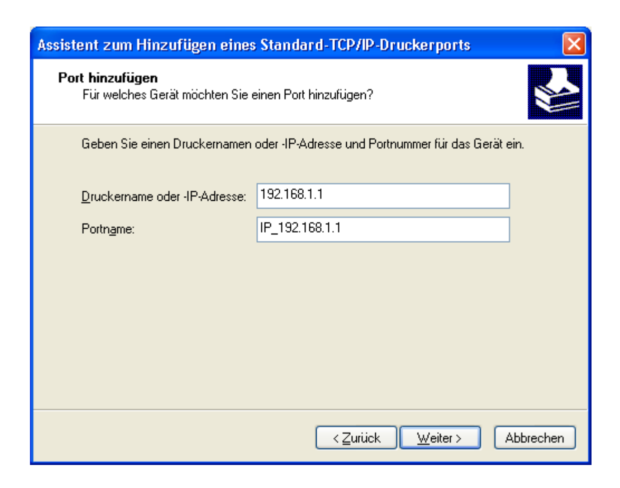
4. Klicken Sie auf "Lokaler Drucker, der an den Computer angeschlossen ist".



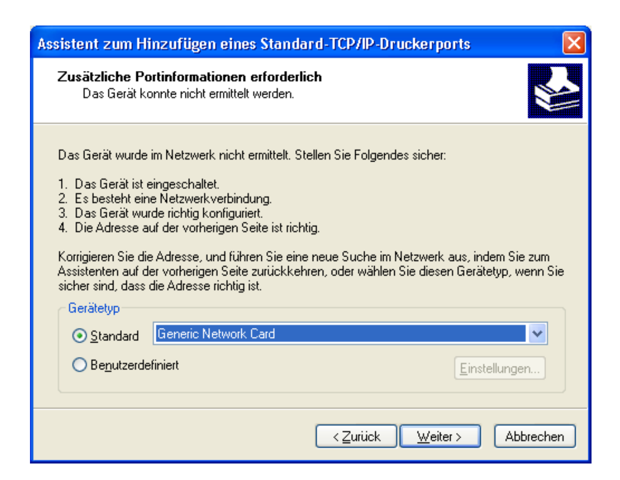
5. Wählen Sie in diesem Dialog **Einen neuen Anschluss erstellen** und markieren Sie in der Dropdown-Liste **Standard TCP/IP Port**. Klicken Sie auf **Weiter**.



6. Geben Sie im folgenden Dialog im Feld **Druckername oder -IP-Adresse** die LAN IP-Nummer des Routers **192.168.1.1** und im Feld **Portname** die Bezeichnung **IP_192.168.1.1** ein. Klicken Sie dann auf **Weiter**.



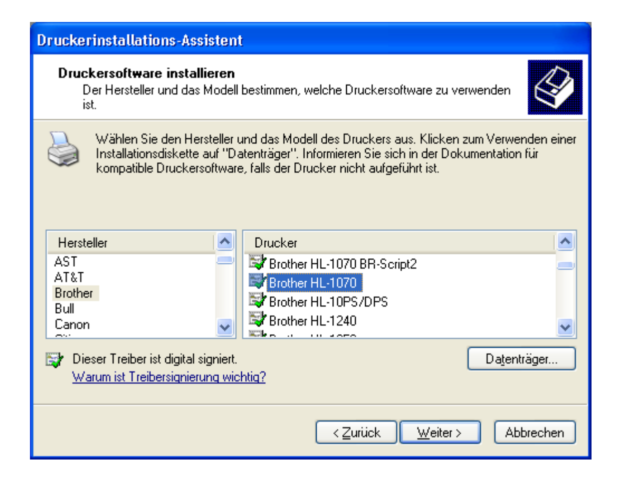
7. Markieren Sie "Standard" und wählen Sie "Generic Network Card".



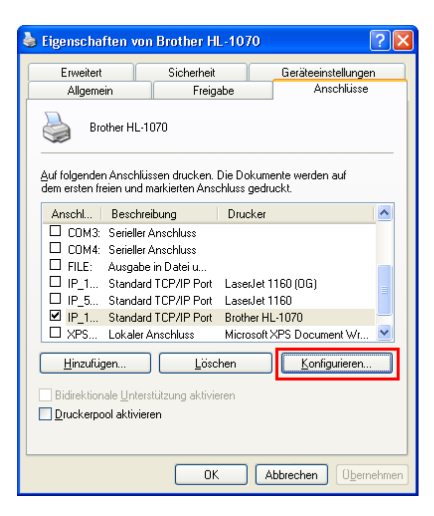
8. Klicken Sie im folgenden Dialog auf **Fertig stellen**.



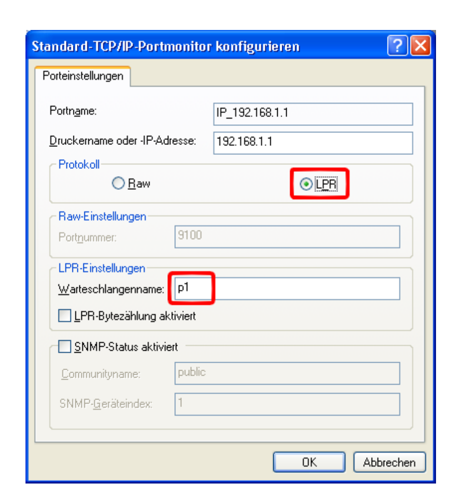
9. Nun fordert Ihr System Sie auf, den richtigen Namen des Druckers zu wählen, den Sie an Ihrem Router angeschlossen haben. Durch diesen Schritt wird der richtiger Treiber auf Ihrem PC geladen. Wählen Sie den Drucker aus und klicken auf **Weiter**.



10. Abschließend müssen Sie in das Menü **Systemsteuerung-> Drucker und Faxgeräte** zurückkehren und die Eigenschaften des neu hinzugefügten Druckers bearbeiten.



11. Nachdem Sie den Dialog **Eigenschaften** (unter **Datei** oder durch Rechtsklick zu erreichen) geöffnet haben, gehen Sie zu dem Reiter **Anschlüsse** und klicken auf **Konfigurieren**. Wählen Sie als **LPR** als Protokoll und geben Sie **p1** (Nummer 1) als Warteschlangenname ein. Klicken Sie dann auf **OK**. Die entsprechenden Einstellungen sind in der Abbildung rot umrandet.



Der Drucker kann jetzt zum Drucken verwendet werden.

Hinweis 1: Einige Drucker mit Fax-/Scanner- oder anderen Zusatzfunktionen werden nicht unterstützt. Falls Sie sich nicht sicher sind, ob Ihr Drucker unterstützt wird, prüfen Sie bitte die Druckerliste unter www.draytek.com. Öffnen Sie hierzu **Support->FAQ->Printer Server** und klicken Sie auf **What types of printers are compatible with Vigor router?**.



Hinweis 2: Der Vigor-Router nimmt Druckaufträge von Rechnern über LAN-Ports an, nicht aber über den WAN-Port.



Grundlegende Einstellungen

Um den Router ordnungsgemäß zu verwenden, ändern Sie zu Ihrer Sicherheit das Web-Konfigurationspasswort und passen Sie die Grundeinstellungen an.

2.1 Zweistufiges Management

Dieses Kapitel erklärt, wie Sie ein Administrator-/Benutzerpasswort einrichten und die grundlegenden/erweiterten Einstellungen für den Zugriff auf das Internet erfolgreich anpassen können.

Für den Benutzermodus geben Sie nichts ein und klicken auf **Anmelden**, um auf die Web-Seiten für die grundlegende Konfiguration zu gelangen. Für den Administratormodus geben Sie unter Benutzername/Passwort "***admin/admin***" ein und klicken auf **Anmelden**, um zur vollen Konfiguration zu gelangen.

2.2 Zugriff auf die Web-Seite

1. Sorgen Sie dafür, dass Ihr PC richtig mit dem Router verbunden ist.



Hinweis: Sie können Ihren Rechner so konfigurieren, dass die IP dynamisch vom Router zugewiesen wird, oder eine IP-Adresse aus dem gleichen Subnetz wählen, in dem sich **die Standard-IP-Adresse des Vigor-Routers befindet (192.168.1.1)**. Einzelheiten hierzu werden im Abschnitt "Fehlerbehandlung" weiter hinten im Handbuch beschrieben.

2. Starten Sie auf Ihrem PC einen Web-Browser und geben Sie **http://192.168.1.1** ein. Das folgende Fenster erscheint und fragt den Benutzernamen und das Passwort ab.

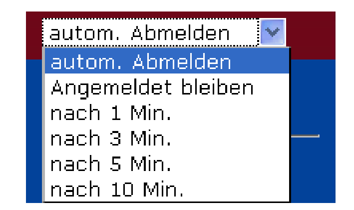


3. Für den Benutzermodus geben Sie nichts ein und klicken auf **Anmelden**, um auf die Web-Seiten für die grundlegende Konfiguration zu gelangen. Für den Administratormodus geben Sie unter Benutzername/Passwort "admin/admin" ein und klicken auf **Anmelden**, um zur vollen Konfiguration zu gelangen.



Hinweis: Falls Sie nicht auf die Web-Konfiguration zugreifen können, sehen Sie bitte im Abschnitt "Fehlerbehandlung" nach, wie Sie das Problem identifizieren und beheben können.

4. Die Abmeldung von der Web-Seite findet gemäß der gewählten Einstellung statt. Die Standardeinstellung ist **Automatisch abmelden**, was bedeutet, dass das Web-Konfigurationssystem automatisch abgemeldet wird, nachdem es fünf Minuten lang nicht betätigt wurde. Sie können diese Einstellung bei Bedarf ändern.

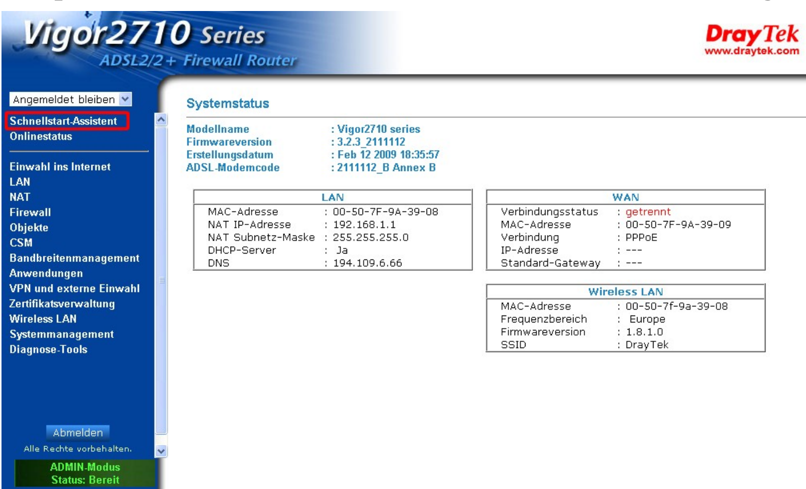


2.3 Passwort ändern

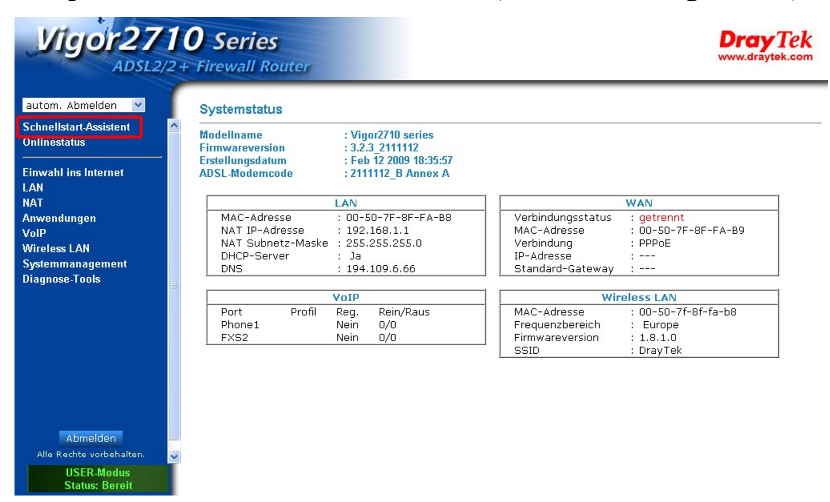
Um die Sicherheit des Routers zu gewährleisten, ändern Sie bitte sowohl das Passwort für den Benutzermodus als auch das Passwort für den Administratormodus.

1. Starten Sie auf Ihrem PC einen Web-Browser und geben Sie **http://192.168.1.1** ein. Ein Popup-Fenster erscheint und fragt den Benutzernamen und das Passwort ab.
2. Für den Administratormodus geben Sie unter Benutzername/Passwort "admin/admin" ein. Andernfalls geben Sie nichts ein (Benutzername und Passwort für den Benutzermodus sind leer) und klicken auf **Anmelden**.
3. Das **Hauptfenster** erscheint.

Hauptfenster für den Administratormodus (erweiterte Konfiguration)

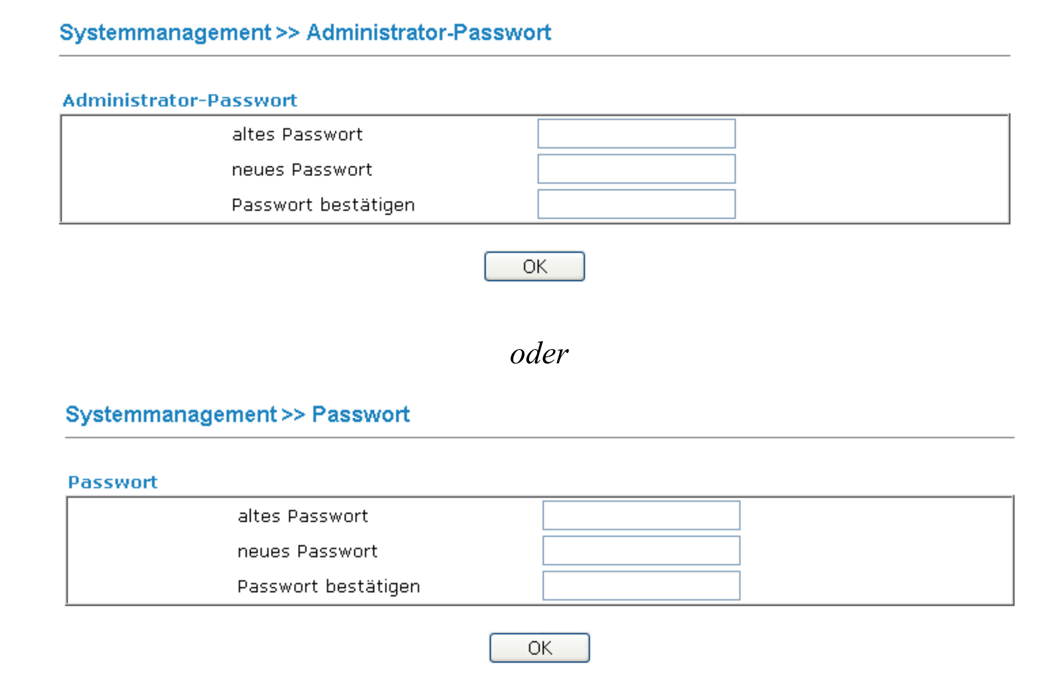


Hauptfenster für den Benutzermodus (einfache Konfiguration)



Anmerkung: Die Startseite kann sich je nach Routermodell leicht unterscheiden.

4. Gehen Sie zu **Systemmanagement** und wählen Sie **Administratorpasswort/Benutzerpasswort**.



5. Geben Sie das Anmeldepasswort (standardmäßig leer) im Feld **Altes Passwort** ein. Geben Sie ein **Neues Passwort** ein. Klicken Sie dann auf **OK**, um fortzufahren.

6. Das Passwort ist nun geändert worden. Verwenden Sie beim nächsten Mal das neue Passwort, um auf das Menü des Routers zuzugreifen.



2.4 Schnellstart-Assistent



Hinweis: Der Schnellstart-Assistent für den Benutzermodus ist mit dem Administratormodus identisch.

Die hier beschriebene Konfiguration wird Sie dabei unterstützen, Ihren Router schnell für Breitband-DSL einzurichten und zu verwenden. Das erste Dialogfenster des **Schnellstart-Assistenten** erfordert die Eingabe des Anmeldepassworts. Geben Sie das Passwort ein und klicken auf **Weiter**.

Schnellstart-Assistent

Login-Passwort eingeben

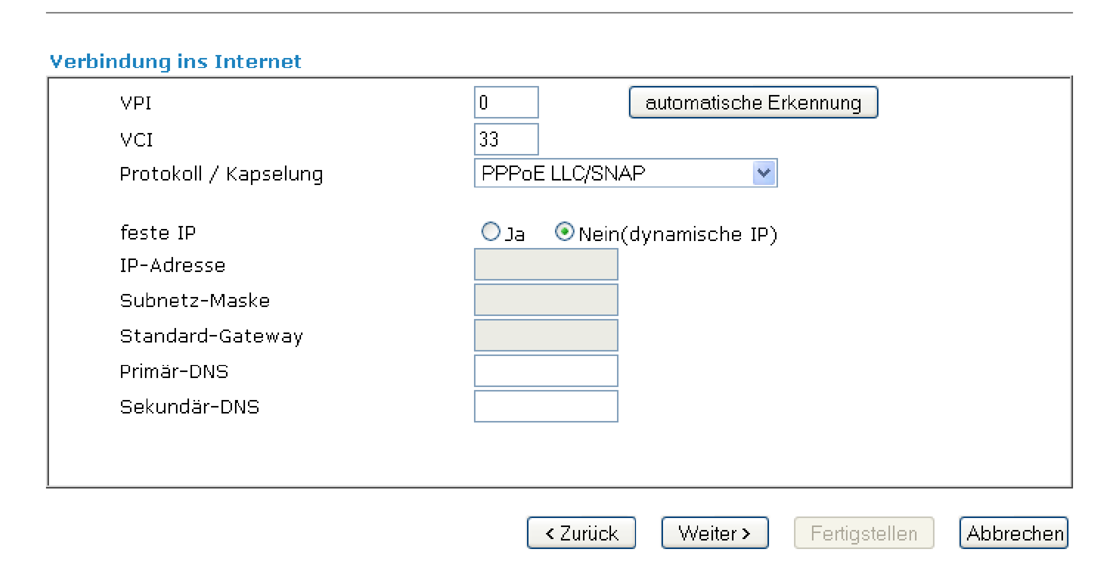
Ab Werk ist kein Passwort voreingestellt. Bitte vergeben Sie zum Schutz Ihrer Konfigurationen eine alpha-numerische Zeichenfolge als Passwort (max. 23 Zeichen).

altes Passwort (falls vorhanden)
neues Passwort
Passwort bestätigen

< Zurück | Weiter > | Fertigstellen | Abbrechen

2.4.1 Auswahl Protokoll/Kapselung

Im **Schnellstart-Assistenten** können Sie den Router über verschiedene Protokolle/Modi wie **PPPoE**, **PPPoA, Bridged IP oder Routed IP** für den Zugriff auf das Internet konfigurieren. Der Router verbindet sich über die ADSL-WAN-Schnittstelle mit dem Internet.



Wählen Sie die richtige WAN-Verbindungsart für die Internet-Verbindung über diesen Router gemäß den von Ihrem ISP mitgeteilten Einstellungen.

VPI — Abkürzung für **Virtual Path Identifier**. Dies ist ein 8-Bit-Header in jeder ATM-Zelle, der angibt, wohin die Zelle geleitet werden soll. ATM ist eine Methode, um Daten in kleinen Paketen fester Größe zu versenden. Es wird verwendet, um Daten auf Client-Rechner zu übertragen.

VCI — Abkürzung für **Virtual Channel Identifier.** Dies ist ein 16-Bit-Feld im Header der ATM-Zelle, welches das nächste Ziel der Zelle auf dem Weg durch das Netzwerk angibt. Ein virtueller Kanal ist eine logische Verbindung zwischen zwei Endgeräten im Netzwerk.

Protokoll/Kapselung — Wählen Sie für diese WAN-Schnittstelle einen Modus. Es sind für den Internetzugang verschiedene Modi verfügbar, z.B. **PPPoE**, **PPPoA, Bridged IP** und **Routed IP**.

Protokoll / Kapselung: PPPoE LLC/SNAP
feste IP
IP-Adresse
Subnetz-Maske
Standard-Gateway
Primär-DNS
Sekundär-DNS

PPPoE LLC/SNAP
PPPoE VC MUX
PPPoA LLC/SNAP
PPPoA VC MUX
1483 Bridged IP LLC
1483 Routed IP LLC
1483 Bridged IP VC-Mux
1483 Routed IP VC-Mux (IPoA)
1483 Bridged IP (IPoE)

Feste IP — Klicken Sie auf **Ja**, um für den Router eine feste IP festzulegen. Andernfalls klicken Sie auf **Nein (dynamische IP)**, um dem Router zu erlauben, eine dynamische IP zu wählen. Falls Sie **Nein** wählen, werden die folgende IP-Adresse, die Subnetz-Maske und das Standard-Gateway nicht geändert.

IP-Adresse — Weisen für das gewählte Protokoll eine IP-Adresse zu.

Subnetz-Maske — Legen Sie für die Protokolle **Routed IP** und **Bridged IP** einen Wert für die Subnetz-Maske fest.

Standard-Gateway — Legen Sie für die Protokolle **Routed IP** und **Bridged IP** eine IP-Adresse für das Standard-Gateway fest.

Primär-DNS — Geben Sie die IP-Adresse des bevorzugten DNS-Servers ein.

Sekundär-DNS — Geben Sie die IP-Adresse des alternativen DNS-Servers ein.

2.4.2 PPPoE/PPPoA

PPPoE ist die Abkürzung für **Point-to-Point Protocol over Ethernet**. Dieses Protokoll verwendet zwei weit verbreitete Standards: PPP und Ethernet. Es verbindet Benutzer per Ethernet über einen gemeinsamen DSL-Anschluss, ein Wireless-Gerät oder ein Kabelmodem mit dem Internet. Alle Benutzer, die über Ethernet verbunden sind, können den Anschluss gemeinsam nutzen.

Die meisten Benutzer eines DSL-Modems verwenden PPPoE. Alle lokalen Benutzer können eine PPPoE-Verbindung für den Zugriff auf das Internet gemeinsam nutzen. Sie erhalten die Informationen zum Benutzernamen, Passwort und Authentifizierungsmodus von Ihrem Internetanbieter.

Falls Ihr ISP die Verbindung über **PPPoE** anbietet, wählen Sie bitte für diesen Router **PPPoE**. Die folgende Seite erscheint:

Schnellstart-Assistent

PPPoE / PPPoA

Benutzername	
Passwort	
Passwort bestätigen	

< Zurück | Weiter > | Fertigstellen | Abbrechen

Benutzername	Geben Sie den von Ihrem ISP mitgeteilten gültigen Benutzernamen ein.
Passwort	Geben Sie das von Ihrem ISB mitgeteilte gültige Passwort ein.
Passwort bestätigen	Passwort erneut eingeben.

Klicken Sie auf **Weiter**, um die Zusammenfassung Ihrer Verbindungseinstellungen zu kontrollieren.

Schnellstart-Assistent

Bitte bestätigen Sie Ihre Eingaben:

VPI:	0
VCI:	33
Protokoll / Kapselung:	PPPoE / LLC
feste IP:	Nein
Primär-DNS:	
Sekundär-DNS:	

< Zurück | Weiter > | Fertigstellen | Abbrechen

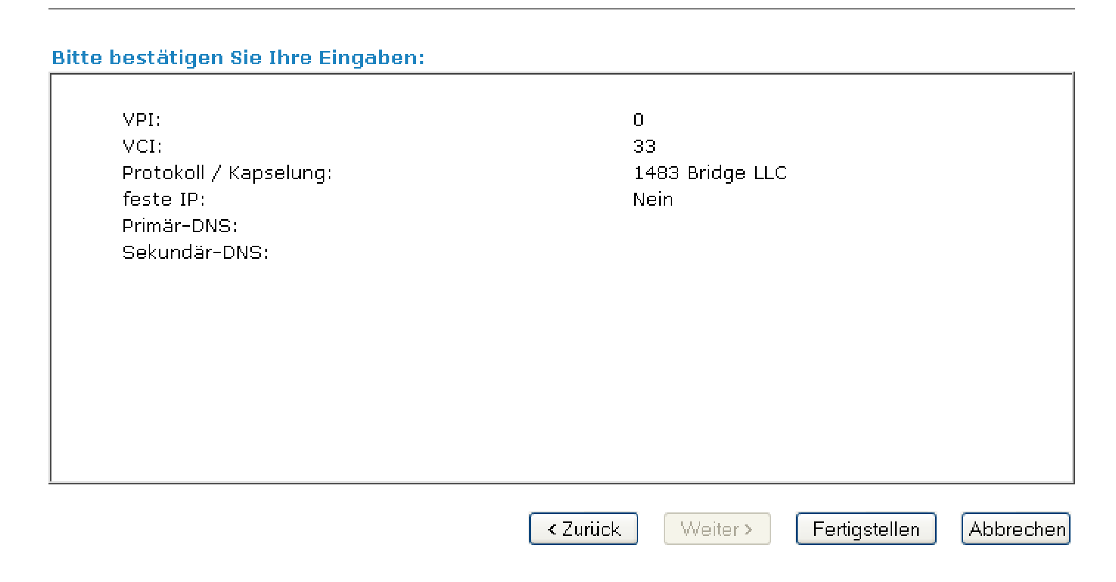
Klicken Sie auf **Fertigstellen**. Der Systemstatus wird angezeigt.

2.4.3 1483 Bridged IP

Wählen Sie **1483 Bridged IP** als Protokoll. Geben Sie alle Daten ein, die Ihnen Ihr ISP für dieses Protokoll mitgeteilt hat.

Klicken Sie auf **Weiter**, um die Zusammenfassung Ihrer Verbindungseinstellungen zu kontrollieren.

Schnellstart-Assistent

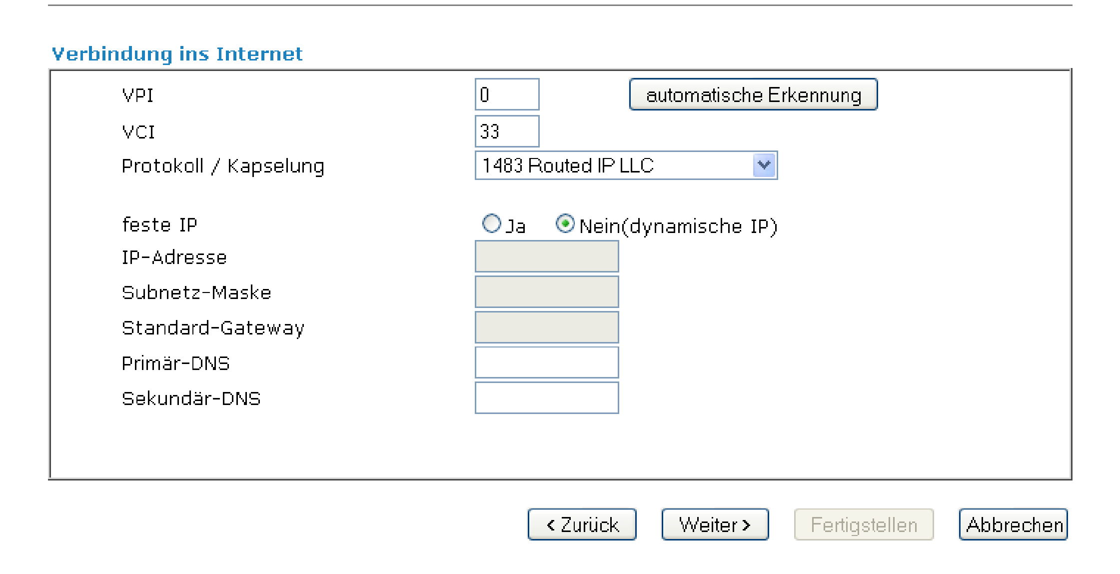


Klicken Sie auf **Fertigstellen**. Der Systemstatus wird angezeigt.

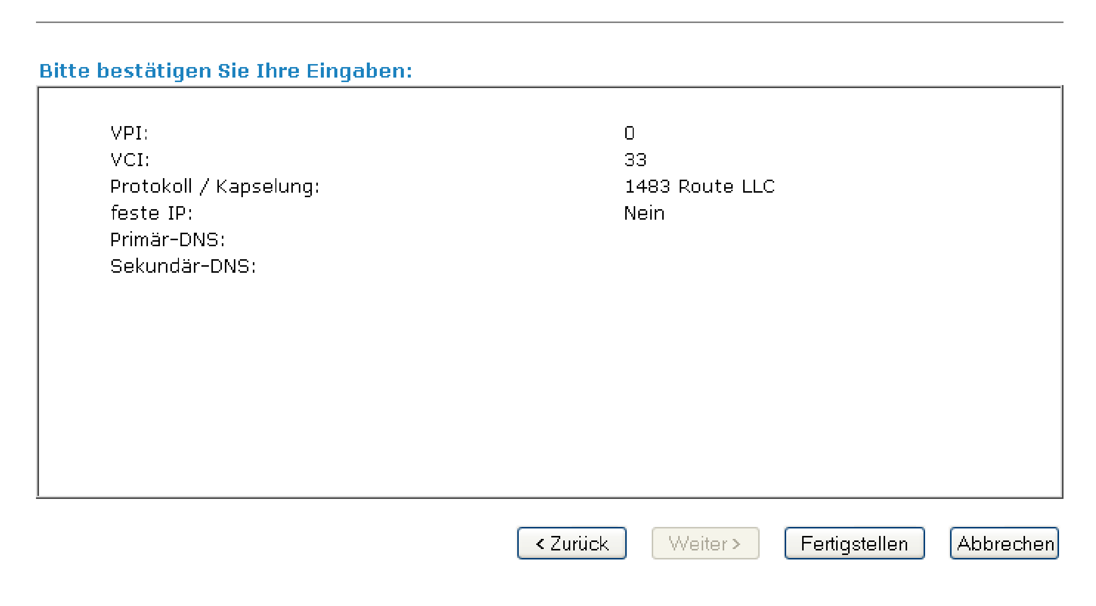
2.4.4 1483 Routed IP

Wählen Sie **1483 Routed IP** als Protokoll. Geben Sie alle Daten ein, die Ihnen Ihr ISP für dieses Protokoll mitgeteilt hat.

Schnellstart-Assistent



Nach Abschluss der Einstellungen auf dieser Seite klicken Sie auf **Weiter**, um zur folgenden Seite zu gelangen.



Klicken Sie auf **Fertigstellen**. Der Systemstatus wird angezeigt.

2.5 Onlinestatus

Der Onlinestatus zeigt den Systemstatus, den WAN-Status, ADSL-Informationen und andere Statusinformationen für den Router auf einer Seite an. Falls Sie **PPPoE/PPPoA** als Protokoll wählen, enthält die Web-Seite, die den Onlinestatus anzeigt, einen Link für **PPPoE wählen** oder **PPPoE trennen**.

Onlinestatus für PPPoE

Online Status

System Status — System Uptime: 0:1:58

Primary | Secondary

LAN Status — Primary DNS: 168.95.192.1 — Secondary DNS: 168.95.1.1

IP Address	TX Packets	RX Packets
192.168.1.5	404	391

WAN 1 Status — >> Drop PPPoE

Enable	Line	Name	Mode	Up Time	
Yes	ADSL		PPPoE	0:01:29	
IP	**GW IP**	**TX Packets**	**TX Rate(Bps)**	**RX Packets**	**RX Rate(Bps)**
61.230.203.119	61.230.192.254	38	15	39	40

ADSL Information (ADSL Firmware Version: 211801_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	63	353	6	1

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	G.DMT	SHOWTIME	256000	2048000	23	31

Onlinestatus für feste IP

Online Status

System Status — System Uptime: 0:1:16

Primary | Secondary

LAN Status		Primary DNS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets	
192.168.1.5	585	500	

WAN 1 Status					
Enable	Line	Name	Mode	Up Time	
Yes	ADSL		Static IP	0:00:28	
IP	GW IP	TX Packets	TX Rate(Bps)	RX Packets	RX Rate(Bps)
192.168.33.12	192.168.33.1	2	4	1	9

ADSL Information (ADSL Firmware Version: 211801_A)

ATM Statistics	TX Blocks	RX Blocks	Corrected Blocks	Uncorrected Blocks
	6	9	0	18

ADSL Status	Mode	State	Up Speed	Down Speed	SNR Margin	Loop Att.
	ADSL2+ (G.992.5)	SHOWTIME	1026000	22215000	6	0

Es folgt eine detaillierte Erläuterung der Angaben:

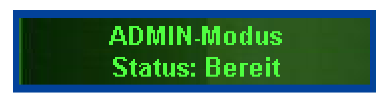
Primär-DNS	Zeigt die IP-Adresse des bevorzugten DNS-Servers an.
Sekundär-DNS	Zeigt die IP-Adresse des alternativen DNS-Servers an.
LAN-Status	
IP-Adresse	Zeigt die IP-Adresse der LAN-Schnittstelle an.
TX-Pakete	Zeigt die Gesamtanzahl der an der LAN-Schnittstelle übertragenen Pakete an.
RX-Pakete	Zeigt die Gesamtanzahl der an der LAN-Schnittstelle empfangenen Pakete an.
WAN1-Status	
Anschluss	Zeigt die physische Verbindung (Ethernet) dieser Schnittstelle an.
Name	Zeigt die Bezeichnung an, die auf der WAN1/WAN Web-Seite festgelegt wurde.
Modus	Zeigt die Art der WAN-Verbindung an (z.B. PPPoE).
Verbindung aktiv seit	Zeigt die Gesamtbetriebszeit der Schnittstelle an.
IP	Zeigt die IP-Adresse der WAN-Schnittstelle an.
GW-IP	Zeigt die IP-Adresse des Standard-Gateways an.
TX-Pakete	Zeigt die Gesamtanzahl der an der WAN-Schnittstelle übertragenen Pakete an.
TX-Rate	Zeigt die Geschwindigkeit der an der WAN-Schnittstelle übertragenen Oktette an.
RX-Pakete	Zeigt die Gesamtanzahl der an der WAN-Schnittstelle empfangenen Pakete an.

RX-Rate	Zeigt die Geschwindigkeit der an der WAN-Schnittstelle empfangenen Oktette an.

> **Hinweis:** Wird der Text in grün angezeigt, so deutet dies darauf hin, dass die WAN-Verbindung dieser Schnittstelle (WAN1) für den Zugriff auf das Internet bereit ist; wird der Text in rot angezeigt, so ist die WAN-Verbindung der Schnittstelle (WAN1) nicht für den Zugriff auf das Internet bereit.

2.6 Konfiguration speichern

Jedes Mal, wenn Sie auf der Web-Seite zur Speicherung der Konfiguration **OK** anklicken, werden Systemmeldungen angezeigt.



Bereit gibt an, dass das System zur Eingabe von Einstellungen bereit ist.

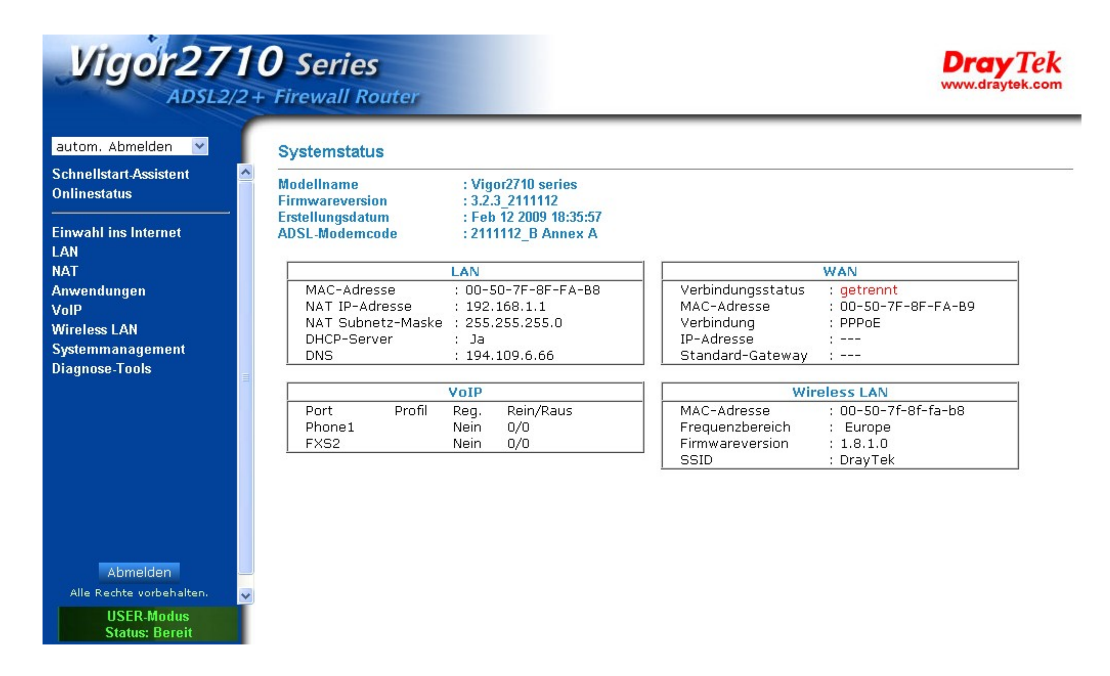
Einstellungen gespeichert bedeutet, dass Ihre Einstellungen gespeichert werden, sobald Sie auf **Fertigstellen** oder **OK** klicken.

3 Benutzermodus

Dieses Kapitel führt Benutzer durch die einfache Konfiguration im Benutzermodus. Weitere Anwendungsfälle werden in Kapitel 5 beschrieben.

1. Starten Sie auf Ihrem PC einen Web-Browser und geben Sie **http://192.168.1.1** ein. Das folgende Fenster erscheint und fragt den Benutzernamen und das Passwort ab.
2. Geben Sie **nichts** ein (Benutzername und Passwort für den Benutzermodus sind leer) und klicken auf **Anmelden**.

Das **Hauptfenster** erscheint. Unten links wird "Benutzermodus" angezeigt.



3.1 Einwahl ins Internet

Der **Schnellstart-Assistent** bietet Benutzern eine einfache Möglichkeit, den Verbindungsmodus für den Router schnell einzurichten. Falls Sie weitere Einstellungen für verschiedene WAN-Modi konfigurieren möchten, gehen Sie bitte ins Menü **WAN** und klicken auf **Einwahl ins Internet**.

3.1.1 Grundlagen des Internet Protocol (IP) Netzwerks

IP ist die Abkürzung für Internet Protocol. Jedes Gerät in einem IP-basierten Netzwerk (z.B. Router, Printserver und Host-PCs) benötigt eine IP-Adresse, welche dessen Standort im Netzwerk bestimmt. Um Adressenkonflikte zu vermeiden, sind IP-Adressen öffentlich beim Network Information Center (NIC) registriert. Eine unverwechselbare IP-Adresse ist für Geräte im öffentlichen Netzwerk unbedingt erforderlich, nicht jedoch in den privaten lokalen TCP/IP-Netzwerken (LANs), da auf diese kein öffentlicher Zugriff nötig ist. Dies können beispielsweise Host-PCs sein, die von einem Router verwaltet werden. Aus diesem Grunde hat das NIC gewisse Adressen reserviert, die niemals öffentlich registriert werden. Diese werden als ***private*** IP-Adressen bezeichnet und umfassen die folgenden Bereiche:

Von 10.0.0.0 bis 10.255.255.255
Von 172.16.0.0 bis 172.31.255.255
Von 192.168.0.0 bis 192.168.255.255

Öffentliche IP-Adressen und private IP-Adressen

Der Router, der für die Verwaltung und den Schutz seines LANs verantwortlich ist, verbindet Gruppen von Host-PCs. Der eingebaute DHCP-Server des Vigor-Routers weist jedem dieser PCs eine private IP-Adresse zu. Der Router selbst verwendet für die Kommunikation mit den lokalen Hosts standardmäßig die **private IP**-Adresse 192.168.1.1. Zur Kommunikation mit anderen Netzwerkgeräten verwendet der Vigor-Router eine **öffentliche IP**-Adresse. Beim Durchfluss der Daten wandelt die Network Address Translation (NAT) Funktion des Routers öffentliche/private Adressen um, und die Pakete werden dem entsprechenden Host-PC im LAN ausgeliefert. Auf diese Weise können alle Host-PCs einen gemeinsamen Internetanschluss nutzen.

Öffentliche IP-Adresse vom ISP beziehen

Beim Einsatz für ADSL muss für eine erfolgreiche Verbindung von Endgeräten PPP-Authentifizierung und Autorisierung verwendet werden. Point-to-Point Protocol over Ethernet (PPPoE) verbindet ein Netzwerk von Hosts über ein Zugriffsgerät mit einem Fernzugriffskonzentrator. Dieser Ansatz vereinfacht die Nutzung für Benutzer. Je nach Benutzeranforderung ermöglicht dies die Zugriffskontrolle, Abrechnung und Angabe der Dienstart (ToS).

Wenn sich ein Router mit Ihrem ISP verbindet, finden verschiedene Verbindungsprozesse statt, um eine Verbindung anzufordern. Dann wird eine Sitzung aufgebaut. Ihr Benutzername und Ihr Passwort werden über **PAP** oder **CHAP** mit dem **RADIUS**-Authentifizierungssystem authentifiziert. Normalerweise werden die IP-Adresse, die DNS-Server und andere Informationen vom ISP zugewiesen.

Die folgende Abbildung zeigt die Menüeinträge für die Einwahl ins Internet:

Einwahl ins Internet
- PPPoE / PPPoA
- MPoA

3.1.2 PPPoE/PPPoA

PPPoA (beschrieben in RFC1483) kann entweder mit dem LLC-Subnetzwerkzugangsprotokoll oder im VC-Mux-Modus verwendet werden. Als Endgerät kapselt der Vigor-Router die PPP-Sitzung für den Transport über die ADSL-Leitung und die DSL-Vermittlungsstelle (DSLAM) Ihres ISPs.

Um PPPoE oder PPPoA als Zugangsprotokoll für das Internet zu verwenden, wählen Sie **PPPoE/PPPoA** im Menü **Einwahl ins Internet**. Die folgende Web-Seite erscheint:

Einwahl ins Internet >> PPPoE / PPPoA

PPPoE / PPPoA Einstellungen

PPPoE/PPPoA ⦿ aktiv ○ inaktiv

DSL-Modem Einstellungen

Multi-PVC Kanal: Kanal 1
VPI: 0
VCI: 33
Kapselung: LLC/SNAP
Protokoll: PPPoE
Modulation: Multimode

PPPoE-Weiterleitung für

☐ kabelgebundenes LAN
☐ Wireless LAN

ISP-Einstellungen

Name des Anbieters
Benutzername
Passwort
PPP-Authentifizierung: PAP oder CHAP
☑ immer in Betrieb
Max. Leerlaufzeit: -1 Sekunden

IP-Adresse des Anbieters [WAN-IP Alias]

feste IP ○ Ja ⦿ Nein (dynamische IP)
feste IP-Adresse

⦿ Voreingestellte MAC-Adresse verwenden
○ MAC-Adresse selbst definieren
MAC-Adresse: 00 : 50 : 7F : 8F : FA : B9

Index (1-15) aus der Verbindungstimer Konfiguration:
=> , , ,

OK

Aktiv/Inaktiv

Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

DSL-Modemeinstellungen

Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind unerlässlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.
Multi-PVC-Kanal - Die hier angezeigte Auswahl wird von der Seite **Einwahl ins Internet** – **Multi PVC** bestimmt. **M-PVC-Kanal auswählen** bedeutet, dass keine Auswahl markiert wird.
VPI - Geben Sie den vom ISP mitgeteilten Wert ein.
VCI - Geben Sie den vom ISP mitgeteilten Wert ein.
Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.
Protokoll - Dropdown-Liste zur Auswahl des vom ISP bestimmten Protokolls.
Falls Sie das Protokoll bereits mit dem **Schnellstart-Assistent**en eingestellt haben, brauchen Sie hier keine Einstellungen zu ändern.

PPPoE Pass-Through

Der Router bietet die Möglichkeit, eine PPPoE-Wählverbindung einzurichten. Außerdem können Sie die PPPoE-Verbindung über den Vigor-Router direkt von den lokalen Clients zum ISP aufbauen. Falls das PPPoA-Protokoll ausgewählt ist, wird das vom PC übertragene PPPoE-Paket in ein PPPoA-Paket umgewandelt und an den WAN-Server übermittelt. Über diese Weiterleitung kann der PC auf das Internet zugreifen.
Kabelgebundenes LAN – Falls Sie dieses Kästchen markieren, können PCs im gleichen Netzwerk für den Internetzugang eine andere PPPoE-Sitzung verwenden (anders als ein Host-PC).
Wireless LAN – Falls Sie dieses Kästchen markieren, können PCs im gleichen Wireless-Netzwerk für den Internetzugang eine

andere PPPoE-Sitzung verwenden (anders als ein Host-PC).

ISP-Einstellungen

Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen, das Passwort und sonstige Authentisierungsparameter ein. Falls Sie ständig mit dem Internet verbunden sein möchten, wählen Sie **Immer in Betrieb**.

Benutzername – Geben Sie den vom ISP mitgeteilten Benutzernamen in diesem Feld ein.

Passwort – Geben Sie das vom ISP mitgeteilte Passwort in diesem Feld ein.

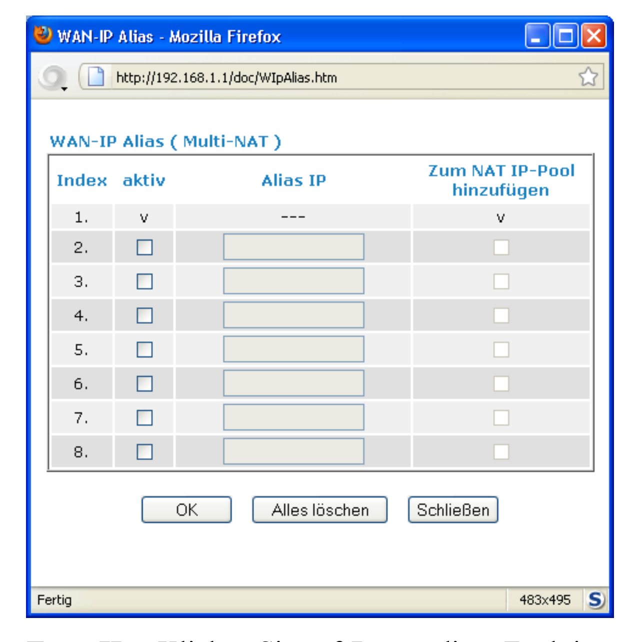
PPP-Authentifizierung – Wählen Sie für PPP entweder **Nur PAP** oder **PAP oder CHAP**.

Max. Leerlaufzeit – Stellen Sie die Leerlaufzeit ein, nach der die Internet-Verbindung abgebrochen werden soll. Diese Einstellung ist nur aktiv, wenn die Betriebsart **Aktiv nach Bedarf** unter **WAN>> Basiskonfiguration** gewählt ist.

IP-Adresse vom ISP

Normalerweise weist der ISP Ihnen dynamisch IP-Adressen zu, wenn Sie sich verbinden und eine Anforderung senden. Einige ISPs bieten einen Service, wobei Sie bei jeder Anforderung die gleiche IP-Adresse zugewiesen bekommen können. In diesem Fall können Sie diese IP-Adresse im Feld **Feste IP** eintragen. Bitte wenden Sie sich an Ihren ISP, bevor Sie diese Funktion verwenden.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen **Aktiv**. Dann klicken Sie auf **OK**, um den Dialog zu verlassen.



Feste IP – Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld **Feste IP-Adresse** eine feste IP-Adresse ein.

Standard-MAC-Adresse – Sie können entweder die **Standard-MAC-Adresse** verwenden oder im entsprechenden Feld eine andere MAC-Adresse für den Router angeben.

MAC-Adresse selbst definieren – Geben Sie die MAC-Adresse für den Router manuell ein.

Index (1-15) in Timerkonfiguration - Sie können für Ihre Anforderungen vier Timer einrichten. Alle Timer können im Voraus auf der Web-Seite **Anwendungen – Timer** eingestellt werden, und Sie können die Nummer verwenden, die Sie auf jener Web-Seite gesetzt haben.

Nach Abschluss aller Einstellungen klicken Sie auf **OK**, um diese zu aktivieren.

MPoA

MPoA ist eine Spezifikation, welche die Integration von ATM-Diensten in bestehenden LANs ermöglicht, die als Protokoll entweder Ethernet oder TCP/IP verwenden. Das Ziel von MPoA ist, verschiedene LANs zu befähigen, einander über ein ATM-Backbone Pakete zu senden.

Um **MPoA** als das Zugriffsprotokoll des Internets zu verwenden, wählen Sie den **MPoA**-Modus. Die folgende Web-Seite erscheint:

Einwahl ins Internet >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Einstellungen

MPoA ○ aktiv ◉ inaktiv

DSL-Modem Einstellungen
Multi-PVC Kanal: Kanal 1
Kapselung: 1483 Bridged IP LLC
VPI: 0
VCI: 33
Modulation: Multimode

RIP-Protokoll
☐ aktiv

Bridge-Modus
☐ aktiv

WAN-IP Netzwerk-Einstellungen
○ Automatisches Beziehen einer IP-Adresse
Router-Name *
Domain-Name *
*: wird von einigen Anbietern benötigt
◉ IP-Adresse definieren [WAN-IP Alias]
IP-Adresse: 0.0.0.0
Subnetz-Maske: 0.0.0.0
Gateway IP-Adresse: 0.0.0.0

◉ Voreingestellte MAC-Adresse verwenden
○ MAC-Adresse selbst definieren
MAC-Adresse: 00 : 50 : 7F : 8F : FA : B9

DNS-Server-IP
Primäre IP-Adresse
Sekundäre IP-Adresse

OK

MPoA (RFC1483/2684) Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

DSL-Modemeinstellungen Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind unerlässlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.

Multi-PVC-Kanal - Die hier angezeigte Auswahl wird von der Seite **Einwahl ins Internet – Multi PVC** bestimmt. **M-PVC-Kanal auswählen** bedeutet, dass keine Auswahl markiert wird.

Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.

VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

RIP-Protokoll

RIP ist die Abkürzung für Routing Information Protocol (RFC1058), welches bestimmt, wie Router Routing-Tabelleninformationen austauschen. Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren.

Bridge-Modus

Falls Sie **Bridged IP** als Protokoll wählen, können Sie dieses Kästchen markieren, um die Funktion aufzurufen. Der Router wird als Bridge-Modem laufen.

WAN-IP-Netzwerkeinstellungen

Dieses Menü ermöglicht Ihnen, eine IP-Adresse automatisch zu beziehen oder manuell einzugeben.

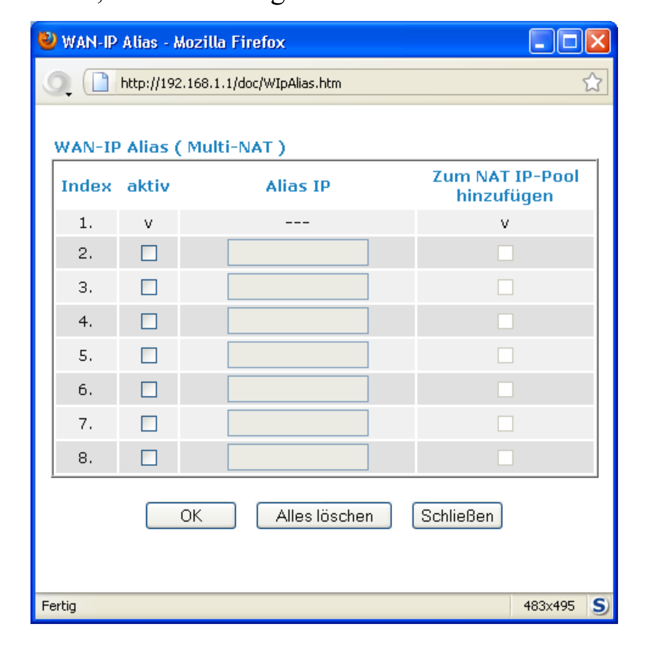
Automatisches Beziehen einer IP-Adresse – Klicken Sie auf diese Taste, um die IP-Adresse automatisch zu beziehen.

Router-Name – Geben Sie den vom ISP mitgeteilten Router-Namen ein.

Domain-Name – Geben Sie den zugewiesenen Domain-Namen ein.

IP-Adresse definieren – Klicken Sie auf diese Taste, um einige Daten einzugeben.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen **Aktiv**. Dann klicken Sie auf **OK**, um den Dialog zu verlassen.



	IP-Adresse – Geben Sie die private IP-Adresse ein.
	Subnetz-Maske – Geben Sie die Subnetz-Maske ein.
	Gateway-IP-Adresse – Geben Sie die IP-Adresse des Gateways ein.
Standard-MAC-Adresse	Geben Sie die MAC-Adresse für den Router ein. Sie können entweder die **Standard-MAC-Adresse** verwenden oder bei Bedarf eine andere MAC-Adresse angeben.
	MAC-Adresse – Geben Sie die MAC-Adresse für den Router manuell ein.
DNS-Server-IP	Geben Sie die bevorzugte IP-Adresse für den Router ein. Falls erforderlich, geben Sie eine alternative IP-Adresse ein.

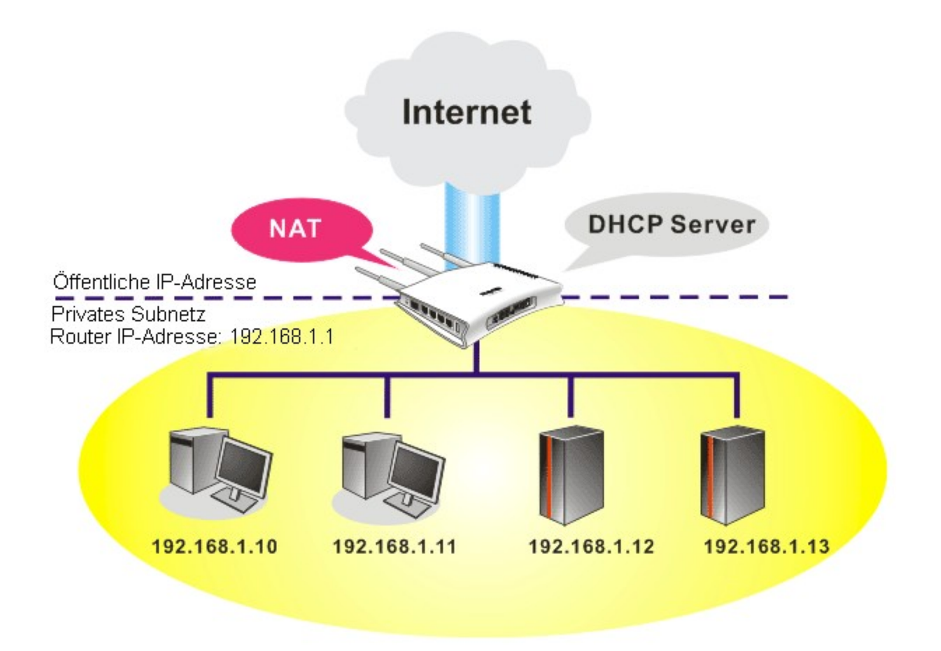
3.2 LAN

Das Local Area Network (LAN) ist eine Gruppe von Subnetzen, die vom Router verwaltet und gesteuert werden. Die Netzwerkstruktur hängt davon ab, welche Art von öffentlichen IP-Adressen Ihnen Ihr ISP zuweist.

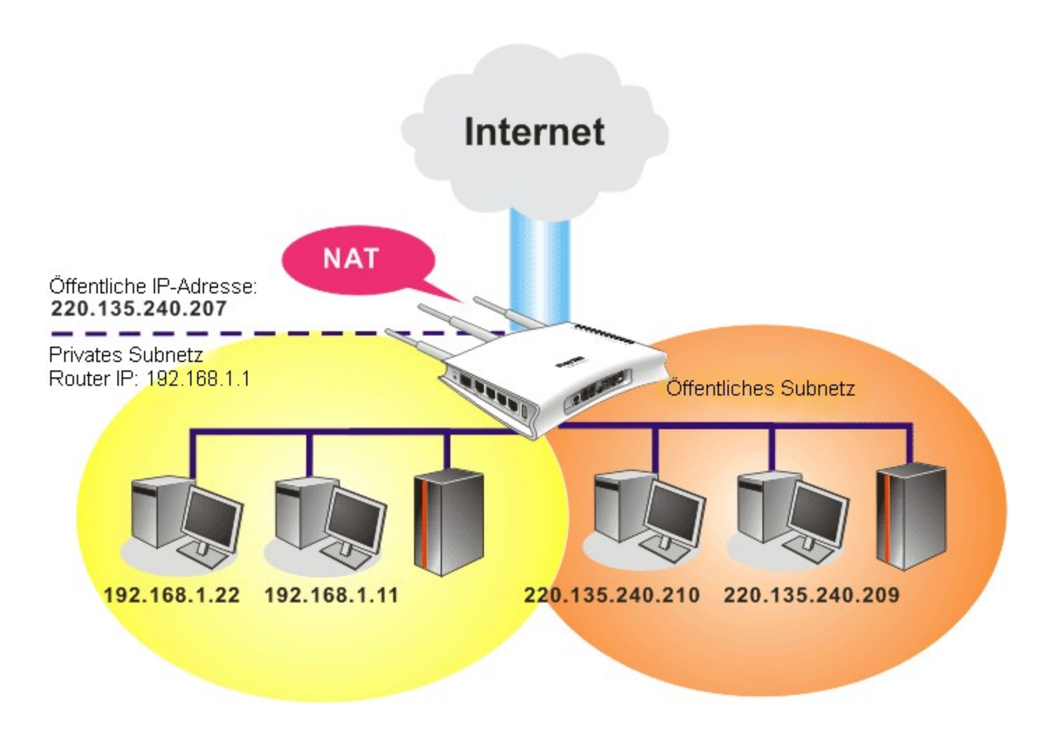


3.2.1 LAN-Grundlagen

Die grundlegende Funktion des Vigor-Routers ist NAT. Hiermit wird ein privates Subnetz aufgebaut. Wie bereits erwähnt, kommuniziert der Router über die öffentliche IP-Adresse mit anderen öffentlichen Hosts im Internet und über die private IP-Adresse mit lokalen Hosts. NAT hat die Aufgabe, die Pakete von der öffentlichen IP-Adresse auf private IP-Adressen umzuschreiben und die entsprechenden Pakete zum richtigen Host und umgekehrt weiterzuleiten. Außerdem verfügt der Vigor-Router über einen eingebauten DHCP-Server, der jedem lokalen Host private IP-Adressen zuweist. Die folgende Abbildung dient dem besseren Verständnis:



In einigen Sonderfällen können Sie von Ihrem ISP ein öffentliches IP-Subnetz wie 220.135.240.0/24 erhalten. Dies bedeutet, dass Sie ein öffentliches Subnetz einrichten können oder ein zweites Subnetz bestimmen können, in dem jeder Host eine öffentliche IP-Adresse erhält. Als Teil des öffentlichen Subnetzes ist der Vigor-Router für das IP-Routing verantwortlich, um Hosts im öffentlichen Subnetz zu ermöglichen, mit anderen öffentlichen Hosts oder Servern zu kommunizieren, die außerhalb liegen. Deswegen sollte der Router als Gateway für öffentliche Hosts eingerichtet werden.



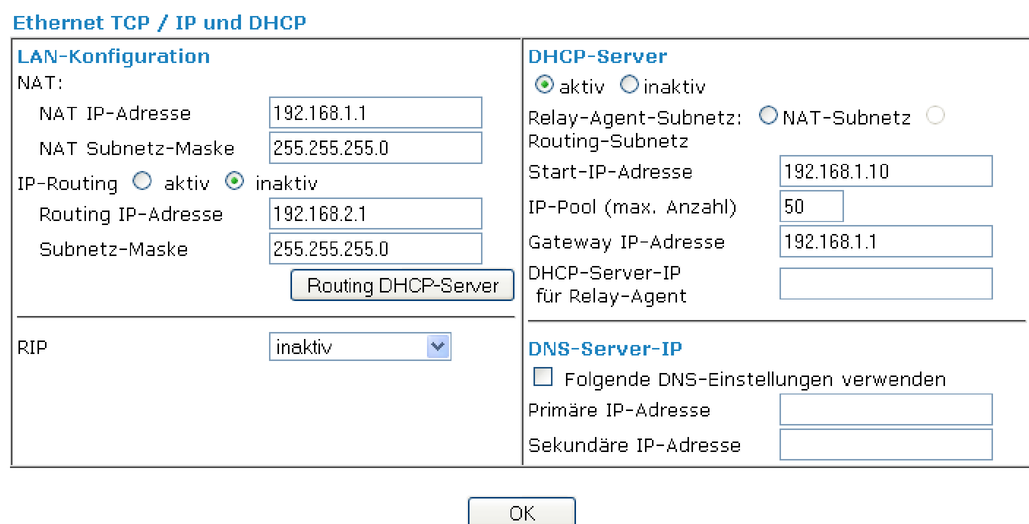
Was ist das Routing Information Protocol (RIP)?

Der Vigor-Router tauscht mit Hilfe von RIP Routing-Informationen mit benachbarten Routern aus, um IP-Routing zu ermöglichen. Auf diese Weise benachrichtigen sich die Router automatisch, wenn Benutzer Daten des Routers ändern, z.B. die IP-Adresse.

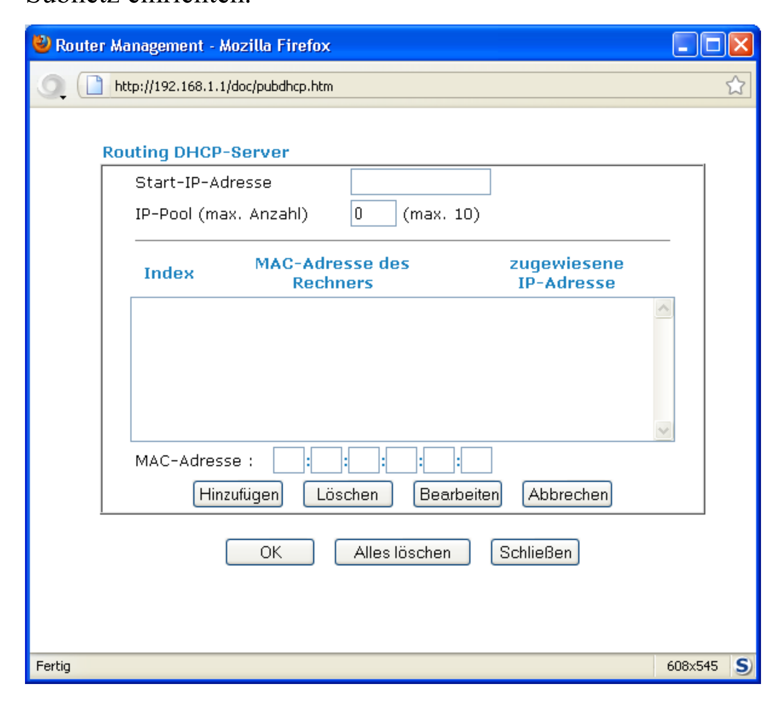
3.2.2 Basiskonfiguration

Diese Seite beinhaltet die allgemeinen LAN-Einstellungen.

Klicken Sie auf **LAN**, um die Seite mit den LAN-Einstellungen zu öffnen, und wählen Sie **Basiskonfiguration**.



NAT IP-Adresse	Geben Sie die private IP-Adresse für die Verbindung zu einem lokalen privaten Netzwerk ein (Standard: 192.168.1.1).
Subnetz-Maske	Geben Sie den Adressbereich ein, der die Größe des Netzwerks bestimmt (Standard: 255.255.255.0/ 24).
IP-Routing	Klicken Sie auf **Aktiv**, um diese Funktion zu starten. Die Standardeinstellung ist **Inaktiv**.
Routing IP-Adresse	Geben Sie die zweite IP-Adresse für die Verbindung zu einem Subnetz ein. (Standard: 192.168.2.1/ 24)
Subnetz-Maske	Ein Adressbereich, der die Größe des Netzwerks bestimmt. (Standard: 255.255.255.0/ 24)
Routing DHCP-Server	Sie können den Router als DHCP-Server für das zweite Subnetz einrichten.



Start-IP-Adresse: Geben Sie einen Wert aus dem IP-Adresspool an, bei dem der DHCP-Server bei der Vergabe von IP-Adressen anfangen soll. Falls die Routing-IP-Adresse Ihres Routers 220.135.240.1 ist, muss die Start-IP-Adresse 220.135.240.2 oder größer, jedoch kleiner als 220.135.240.254 sein.

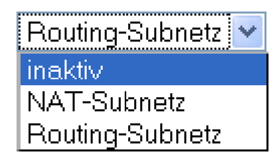
IP-Pool (Anzahl): Geben Sie die Anzahl der IP-Adressen in diesem Pool an. Die maximale Anzahl beträgt 10. Wenn Sie zum Beispiel 3 eingeben und die Routing-IP-Adresse Ihres Routers 220.135.240.1 ist, so reicht der IP-Adressbereich des DHCP-Servers von 220.135.240.2 bis 220.135.240.4.

MAC-Adresse: Geben Sie die MAC-Adressen der Hosts nacheinander ein und klicken Sie auf **Hinzufügen**, um eine Liste der Hosts zu erstellen, denen aus dem oben erwähnten Pool IP-Adressen zugewiesen, gelöscht oder geändert werden sollen. Die Erstellung einer Liste von MAC-Adressen für den Routing-DHCP-Server ermöglicht dem Router, den richtigen Hosts die richtigen IP-Adressen des richtigen Subnetzes zuzuweisen. So

wird vermieden, dass den Hosts im Routing-Subnetz IP-Adressen aus dem NAT-Subnetz zugewiesen werden.

RIP

Inaktiv deaktiviert das RIP-Protokoll. Damit wird zwischen Routern keine Routing-Information ausgetauscht. (Standardeinstellung)



NAT-Subnetz - Lässt den Router die RIP-Information des NAT-Subnetzes mit benachbarten Routern austauschen.

Routing-Subnetz - Lässt den Router die RIP-Information des Routing-Subnetzes mit benachbarten Routern austauschen.

DHCP-Serverkonfiguration

DHCP ist die Abkürzung für Dynamic Host Configuration Protocol. Der Router dient standardmäßig als DHCP-Server für Ihr Netzwerk und sendet automatisch IP-bezogene Einstellungen an alle lokalen Rechner, die als DHCP-Clients konfiguriert sind. Es wird empfohlen, den Router als DHCP-Server aktiviert zu lassen, sofern Sie für Ihr Netzwerk keinen gesonderten DHCP-Server haben.

Falls Sie im Netzwerk nicht den Vigor-Router, sondern einen anderen Rechner als DHCP-Server benutzen möchten, können Sie den Relay-Agent verwenden, um die DHCP-Anforderungen an den jeweiligen Rechner umzuleiten.

Aktiv - Lässt den Router jedem Host im LAN IP-Adressen zuweisen.

Inaktiv – Lässt Sie manuell jedem Host im LAN IP-Adressen zuweisen.

Relay-Agent – (NAT-Subnetz/Routing-Subnetz) Geben Sie das Subnetz an, in dem sich der DHCP-Server befindet, an den der Relay-Agent die DHCP-Anforderungen weiterleiten soll.

Start-IP-Adresse - Geben Sie einen Wert aus dem IP-Adresspool an, bei dem der DHCP-Server bei der Vergabe von IP-Adressen anfangen soll. Falls die erste IP-Adresse Ihres Routers 192.168.1.1 ist, muss die Start-IP-Adresse 192.168.1.2 oder größer, jedoch kleiner als 192.168.1.254 sein.

IP-Pool (Anzahl) - Geben Sie die maximale Anzahl der Rechner an, denen der DHCP-Server IP-Adressen zuweisen soll. Der Standardwert beträgt 50, und die maximale Anzahl ist 253.

Gateway-IP-Adresse - Geben Sie die Gateway-IP-Adresse für den DHCP-Server ein. Der Wert entspricht üblicherweise der ersten IP-Adresse des Routers, d.h. der Router ist das Standard-Gateway.

DHCP-Server-IP für Relay-Agent - Setzen Sie die IP-Adresse des DHCP-Servers, den Sie verwenden möchten, damit der Relay-Agent die DHCP-Anforderungen an diesen DHCP-Server weiterleiten kann.

DNS-Serverkonfiguration

DNS ist die Abkürzung für Domain Name System. Jeder Internet-Host muss eine eindeutige IP-Adresse haben und kann auch einen Namen tragen, der einfach zu merken ist, wie z.B. www.yahoo.com. Der DNS-Server wandelt den benutzerfreundlichen Namen in die entsprechende IP-Adresse um.

Folgende DNS-Einstellungen verwenden - Den Vigor-Router zwingen, nicht die vom Internetzugangsserver bestimmten DNS-Server (PPPoE, PPTP, L2TP oder DHCP-Server), sondern die DNS-Server auf dieser Seite zu verwenden.

Primäre IP-Adresse - Geben Sie hier die IP-Adresse eines DNS-Servers ein, dessen Daten Ihnen Ihr ISP mitgeteilt haben sollte. Falls der ISP diese Daten nicht bereitstellt, trägt der Router automatisch die IP-Adresse des Standard-DNS-Servers in diesem Feld ein: 194.109.6.66.

Sekundäre IP-Adresse - Hier können Sie eine alternative DNS-Server-IP eintragen, falls der ISP Ihnen die Daten mehrerer DNS-Server mitgeteilt hat. Falls der ISP diese Daten nicht bereitstellt, trägt der Router automatisch die IP-Adresse des standardmäßigen alternativen DNS-Servers in diesem Feld ein: 194.98.0.1.

Die Standard-DNS-Server-IP ist unter dem Onlinestatus sichtbar:

System Status — System Uptime: 0:54:34

Primary	Secondary	
LAN Status	Primary DNS: 194.109.6.66	Secondary DNS: 168.95.1.1
IP Address	TX Packets	RX Packets
192.168.1.1	1311	1221

Falls die Felder für die IP-Adressen des bevorzugten DNS-Servers und des alternativen DNS-Servers nicht ausgefüllt werden, weist der Router seine eigene IP-Adresse als DNS-Proxy-Server für lokale Benutzer zu und unterhält einen DNS-Cache.

Falls die IP-Adresse eines Domain-Namens bereits im DNS-Cache vorhanden ist, löst der Router den Domain-Namen sofort auf. Andernfalls leitet der Router die DNS-Anfrage über die WAN-Verbindung (z.B. DSL, Kabel) an den externen DNS-Server weiter.

In Kapitel 4 werden zwei übliche Szenarien für LAN-Einstellungen vorgestellt. Neben Einzelheiten zu den Konfigurationsbeispielen enthält das Kapitel weitere Informationen für Ihre Bedürfnisse.

3.3 NAT

Normalerweise dient der Router als NAT-Router (Network Address Translation). Der NAT-Mechanismus ermöglicht die Verwendung von einer oder mehreren privaten IP-Adressen mit einer öffentlichen IP-Adresse. Die öffentliche IP-Adresse wird gewöhnlich von Ihrem ISP zugewiesen, was kostenpflichtig sein kann. Private IP-Adressen werden nur zwischen internen Hosts erkannt.

Wenn abgehende Pakete, die an einen öffentlichen Server im Internet gerichtet sind, beim NAT-Router ankommen, ändert der Router deren Quelladresse in die öffentliche IP-Adresse des Routers, wählt den verfügbaren Port und leitet die Pakete weiter. Gleichzeitig macht der Router in einer Tabelle einen Eintrag, um sich diese Adress-/Portzuordnung zu merken. Wenn der öffentliche Server antwortet, ist der eingehende Verkehr natürlich an die öffentliche IP-Adresse des Routers gerichtet, weshalb der Router anhand der Tabelle die Umwandlung vornimmt. So ist es einem internen Host möglich, flüssig mit einem externen Host zu kommunizieren.

Einige Vorteile von NAT:

- **Einsparung von Kosten für öffentliche IP-Adressen und effizienter Einsatz der IP-Adresse.** NAT ermöglicht die Übersetzung der internen IP-Adressen lokaler Hosts in eine einzige öffentliche IP-Adresse, so dass für sämtliche interne Hosts lediglich eine IP-Adresse erforderlich ist.
- **Höhere Sicherheit des internen Netzwerks durch Verdeckung der internen IP-Adresse.** Es gibt viele Arten von Angriffen auf Grundlage der IP-Adresse. Da der Angreifer die internen IP-Adressen nicht kennt, stellt die NAT-Funktion einen Schutz für das interne Netzwerk dar.

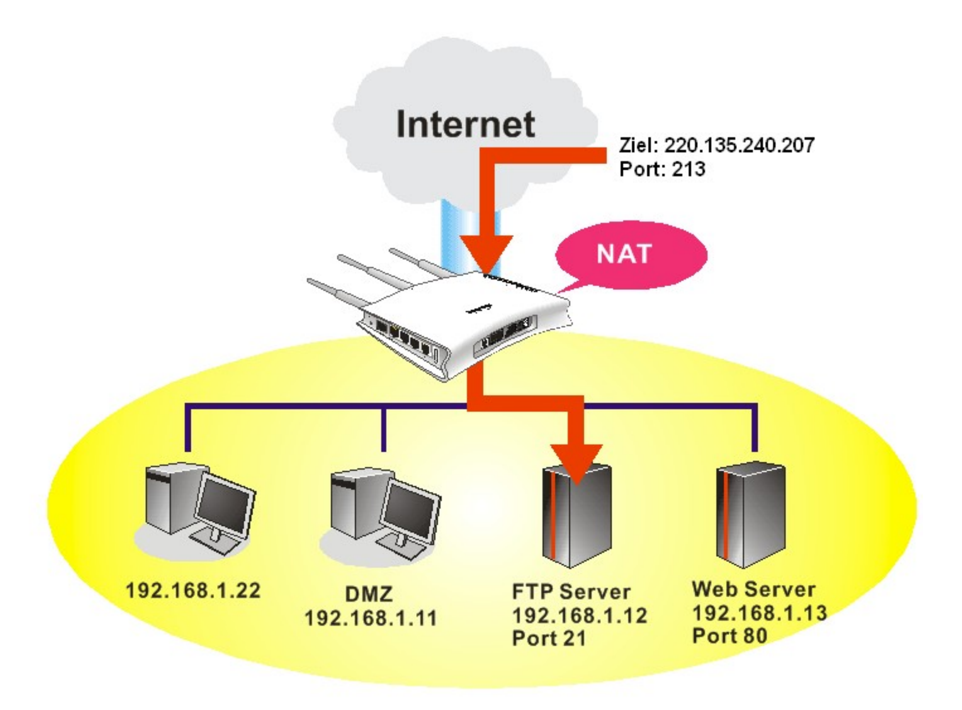
Auf der NAT-Seite sehen Sie die in RFC-1918 definierte private IP-Adresse. Normalerweise wird das Subnetz 192.168.1.0/24 für den Router verwendet. Wie oben erwähnt, kann die NAT-Funktion verschiedenen Diensten eine oder mehrere IP-Adressen oder Ports zuordnen, d.h. die NAT-Funktion verwendet Port-Zuordnungsmethoden.

Die folgende Abbildung zeigt die Menüeinträge für NAT:



3.3.1 Portumleitung

Portumleitung wird gewöhnlich für serverbezogene Dienste im lokalen Netzwerk genutzt, z.B. für Web-Server, FTP-Server, E-Mail-Server, usw. Meistens benötigen Sie für jeden Server eine öffentliche IP-Adresse, und diese öffentliche IP-Adresse/Domain-Name wird von allen Benutzern erkannt. Da der Server sich jedoch innerhalb des LANs befindet, das Netzwerk vom NAT des Routers geschützt wird und unter seiner privaten IP-Adresse/Port identifiziert wird, besteht der Zweck der Portumleitung darin, alle Zugriffe mit öffentlicher IP-Adresse von externen Benutzern an die private IP-Adresse/Port des Servers umzuleiten.



Die Portumleitung ist nur für eingehenden Datenverkehr möglich.

Um diese Funktion zu nutzen, gehen Sie zur **NAT**-Seite und wählen **Portumleitung**. Die **Portumleitungstabelle** ermöglicht 20 Port-Zuordnungseinträge für die internen Hosts.

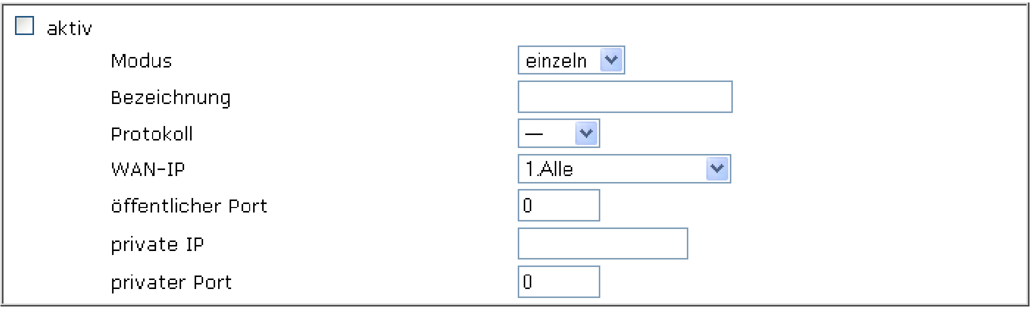
NAT >> Portumleitung

Portumleitung | Auf Werkseinstellungen zurücksetzen |

Index	Bezeichnung	öffentlicher Port	private IP	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 >> Weiter >>

Klicken Sie auf eine beliebige Nummer unter "Index", um auf die nächste Seite für die Konfiguration der Portumleitung zu gelangen.



Aktiv Markieren Sie dieses Kästchen, um die Portumleitung zu aktivieren.

Modus Es stehen hier zwei Optionen (**Einzeln** und **Bereich**) zur Auswahl. Um für den Dienst einen Bereich zu bestimmen, wählen Sie **Bereich**. Bei Eingabe der öffentlichen Ports (Startport und Endport) und der Start-IP des privaten IP-Adressbereichs im Bereichsmodus berechnet das System automatisch die End-IP des privaten IP-Adressbereichs und zeigt diese an.

Bezeichnung Geben Sie eine Beschreibung des jeweiligen Netzwerkdienstes ein.

Protokoll Wählen Sie das Protokoll für die Transportschicht (TCP oder UDP).

WAN-IP Bestimmen Sie die WAN-IP für die Portumleitung. Es stehen acht IP-Aliasse zur Auswahl, die für die Portumleitung verwendet werden können. Die Standardeinstellung ist **Alle**, was bedeutet, dass sämtliche eingehende Daten von jedem Port zum angegebenen IP-Adress- und Portbereich weitergeleitet werden.

Öffentlicher Port Geben Sie an, welcher Port an die angegebene **private IP und Port** des internen Hosts umgeleitet werden soll. Falls Sie **Bereich** als Portumleitungsmodus wählen, sehen Sie in diesem Feld zwei Kästchen. Geben Sie die gewünschte Nummer im ersten Kästchen ein. Das zweite Kästchen wird danach automatisch ausgefüllt.

Private IP Geben Sie die private IP-Adresse des internen Hosts an, der den Dienst anbietet. Falls Sie **Bereich** als Portumleitungsmodus wählen, sehen Sie in diesem Feld zwei Kästchen. Geben Sie im ersten Kästchen eine komplette IP-Adresse ein (als Anfangspunkt) und die vierte Zifferngruppe im zweiten Kästchen (als Endpunkt).

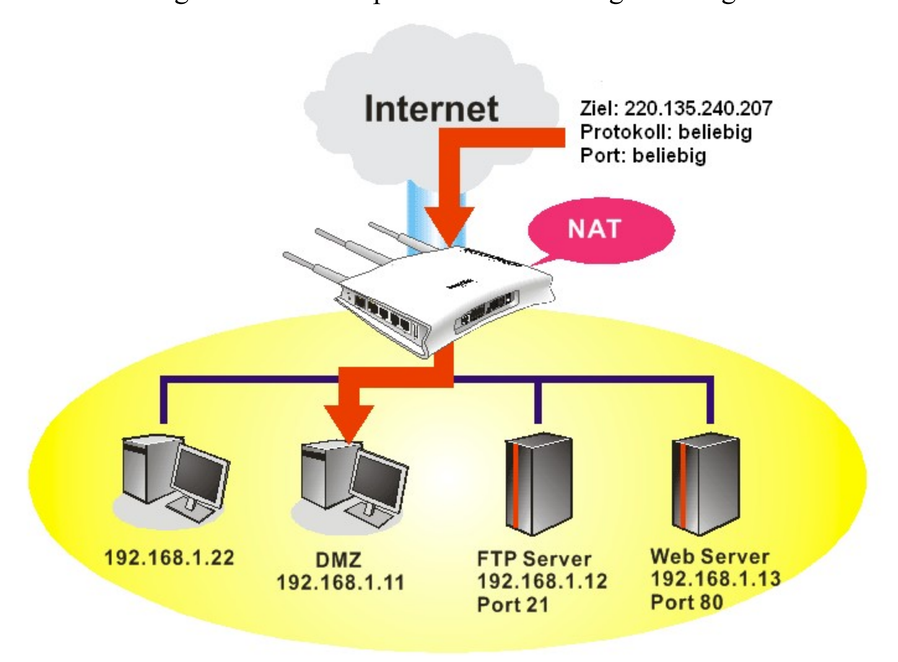
Privater Port Geben Sie die private Portnummer des Dienstes an, den der interne Host anbietet.

Aktiv Markieren Sie dieses Kästchen, um die definierte Port-Zuordnung zu aktivieren.

Beachten Sie, dass der Router eigene Dienste (Server) wie Telnet, HTTP und FTP hat. Da diese Dienste (Server) immer die gleichen Portnummern verwenden, kann es notwendig sein, die Portnummern des Routers zu ändern, um Konflikte zu vermeiden.

3.3.2 DMZ-Host

Wie oben erwähnt, kann die **Portumleitung** eingehenden TCP-/UDP-Verkehr oder anderen Verkehr auf bestimmten Ports an die angegebene private IP-Adresse/Port des Hosts im LAN umleiten. Es ist jedoch zu beachten, dass andere IP-Protokolle wie z.B. die Protokolle 50 (ESP) und 51 (AH) nicht auf einem festen Port kommunizieren. Der Vigor-Router bietet eine **DMZ-Host**-Funktion, die sämtliche unangeforderte Daten auf beliebigen Protokollen einem einzigen Host im LAN zuordnet. Normales Web-Surfen und andere Internet-Aktivitäten anderer Clients funktionieren weiterhin ohne unangemessene Unterbrechung. **DMZ-Host** ermöglicht einem definierten internen Benutzer, dem Internet vollständig ausgesetzt zu sein, was für gewisse Anwendungen wie Netmeeting oder Internet-Spiele usw. notwendig sein mag.



> Die Sicherheitseigenschaften von NAT werden umgangen, wenn Sie einen DMZ-Host einrichten. Wir empfehlen Ihnen daher, zusätzliche Filterregeln oder eine zweite Firewall zu konfigurieren.

Klicken Sie auf **DMZ-Host**, um die folgende Seite zu öffnen:

NAT >> DMZ-Host

DMZ-Host

WAN1

inaktiv

private IP | PC wählen

MAC-Adresse des True-IP DMZ-Hosts 00 : 00 : 00 : 00 : 00 : 00

Hinweis: Sobald ein True-IP DMZ-Host aktiv ist, wird die WAN-Vebindung immer in Betrieb sein; denn bei True-IP wird die WAN-IP als DMZ-IP verwendet.

OK

Falls Sie zuvor einen **WAN-Alias** für den **PPPoE/PPPoA** oder **MPoA**-Modus eingerichtet haben, finden Sie diesen unter **Alias IP** zur Auswahl.

NAT >> DMZ-Host

DMZ-Host

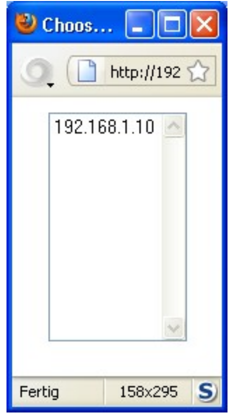
WAN1				
Index	aktiv	Alias IP	private IP	
1.	☐	192.168.1.55		PC wählen

OK Löschen

Aktiv Markieren Sie dieses Kästchen, um die DMZ-Host-Funktion zu aktivieren.

Private IP Geben Sie die private IP-Adresse des DMZ-Hosts ein oder klicken Sie auf "PC wählen", um eine IP-Adresse zu wählen.

PC wählen Wenn Sie auf diese Taste klicken, öffnet sich automatisch das unten abgebildete Fenster. Das Fenster enthält eine Liste privater IP-Adressen aller Hosts in Ihrem LAN. Bestimmen Sie eine private IP-Adresse aus der Liste als DMZ-Host.



Nachdem Sie im gezeigten Dialog eine private IP gewählt haben, wird die IP-Adresse im folgenden Fenster angezeigt. Klicken Sie auf **OK**, um diese Einstellung zu speichern.



3.3.3 Offene Ports

Offene Ports ermöglicht Ihnen, einen Portbereich für den Verkehr besonderer Anwendungen zu öffnen.

Bestimmte Ports müssen beispielsweise für P2P-Anwendungen (BT, KaZaA, Gnutella, WinMX, eMule usw.), Webcam usw. geöffnet werden. Sorgen Sie dafür, dass die betreffende Anwendung immer auf dem neuesten Stand ist, um Angriffe auf eventuelle Sicherheitslücken zu vermeiden.

Klicken Sie auf **Offene Ports**, um die folgende Seite zu öffnen:

NAT >> Offene Ports

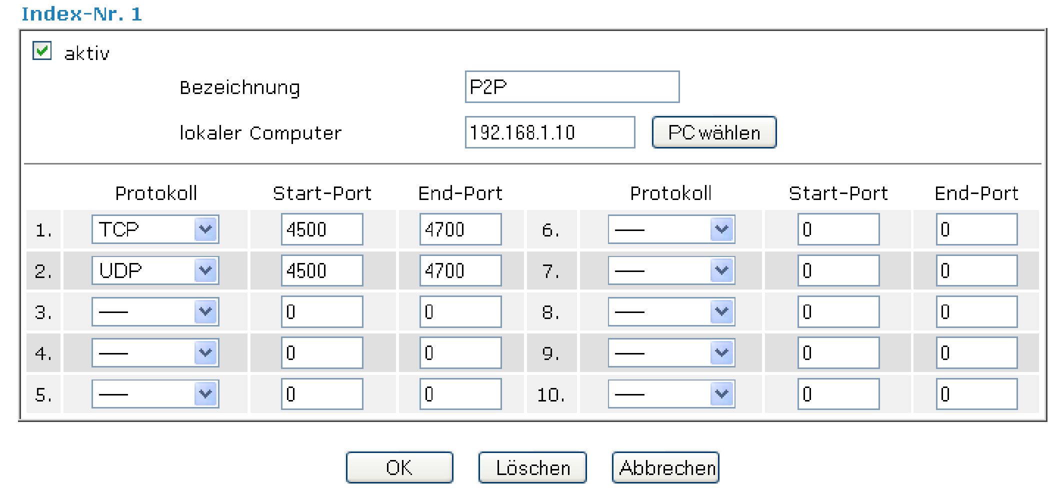
Einstellungen offener Ports | Auf Werkseinstellungen zurücksetzen |

Index	Bezeichnung	Alias IP	lokale IP-Adresse	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 >> Weiter >>

Index	Geben Sie die relative Nummer eines bestimmten Eintrags an, für den Sie einen Dienst auf einem lokalen Host anbieten möchten. Klicken Sie auf die entsprechende Indexnummer, um den Eintrag zu bearbeiten oder zu löschen.
Bezeichnung	Geben Sie die Bezeichnung des definierten Netzwerkdienstes an.
Lokale IP-Adresse	Private IP-Adresse des lokalen Hosts anzeigen, der den Dienst anbietet.
Status	Status des entsprechenden Eintrags anzeigen. X oder V steht für **Inaktiv** bzw. **Aktiv**.

Um Porteinstellungen hinzuzufügen oder zu bearbeiten, klicken Sie auf eine der Indexnummern auf der Seite. Die Konfigurationsseite für den Indexeintrag erscheint. In jedem Indexeintrag können Sie **10** Portbereiche für verschiedene Dienste angeben.



Aktiv Markieren Sie dieses Kästchen, um diesen Eintrag zu aktivieren.

Bezeichnung Geben Sie die Bezeichnung der definierten Netzwerkanwendung/des definierten Netzwerkdienstes an.

WAN-Schnittstelle Geben Sie die WAN-Schnittstelle an, die für diesen Eintrag verwendet werden soll.

Lokaler Computer Geben Sie die private IP-Adresse des lokalen Hosts ein oder klicken Sie auf **PC wählen**, um eine IP-Adresse zu wählen.

PC wählen Wenn Sie auf diese Taste klicken, öffnet sich automatisch ein Fenster mit einer Liste privater IP-Adressen von lokalen Hosts. Wählen Sie die entsprechende IP-Adresse des lokalen Hosts aus der Liste.

Protokoll Wählen Sie das Protokoll für die Transportschicht. Zur Auswahl stehen **TCP**, **UDP** oder **-----** (keines).

Start-Port Geben Sie die Start-Portnummer des Dienstes an, den der interne Host anbietet.

End-Port Geben Sie die End-Portnummer des Dienstes an, den der interne Host anbietet.

3.4 Anwendungen

Die folgende Abbildung zeigt die Menüeinträge für Anwendungen:



3.4.1 Dynamisches DNS

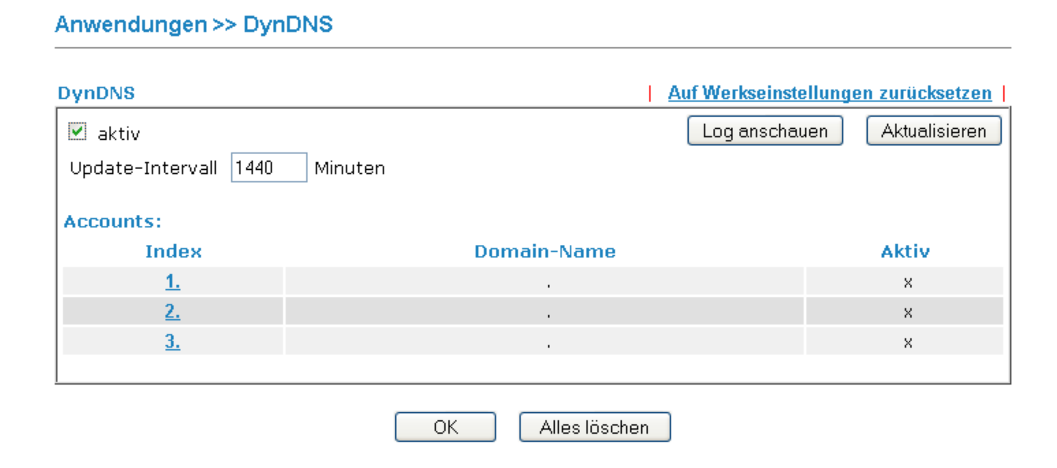
Der ISP weist Ihnen meistens eine dynamische IP-Adresse zu, mit der Sie sich über Ihren ISP mit dem Internet verbinden können. Dies bedeutet, dass sich die Ihrem Router zugewiesene öffentliche IP-Adresse in gewissen Abständen ändert. Die dynamische DNS-Funktion ermöglicht Ihnen, einer dynamischen WAN-IP-Adresse einen Domain-Namen zuzuweisen. So kann der Router seine Online-WAN-IP-Adresszuweisungen auf dem angegebenen DDNS-Server aktualisieren. Wenn der Router online ist, ist es möglich, anhand des registrierten Domain-Namens aus dem Internet auf den Router oder auf die internen virtuellen Server zuzugreifen. Dies ist besonders dann sinnvoll, wenn Sie hinter dem Router einen Web-Server, FTP-Server oder andere Server betreiben.

Bevor Sie die dynamische DNS-Funktion nutzen können, müssen Sie vom DDNS-Anbieter die Freischaltung des DDNS-Dienstes beantragen. Der Router ermöglicht die Einrichtung von bis zu drei Konten bei drei verschiedenen DDNS-Anbietern. Grundsätzlich sind Vigor-Router mit den DDNS-Diensten der beliebtesten DDNS-Anbieter kompatibel, z.B. **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com.** Besuchen Sie deren Web-Sites, um Ihren Domain-Namen für den Router zu registrieren.

Funktion aktivieren und dynamisches DNS-Konto hinzufügen

1. Nehmen wir an, der bei Ihrem DDNS-Anbieter registrierte Domain-Name ist *hostname.dyndns.org*, und Sie haben ein Konto mit dem Benutzernamen *test* und dem Passwort *test*.

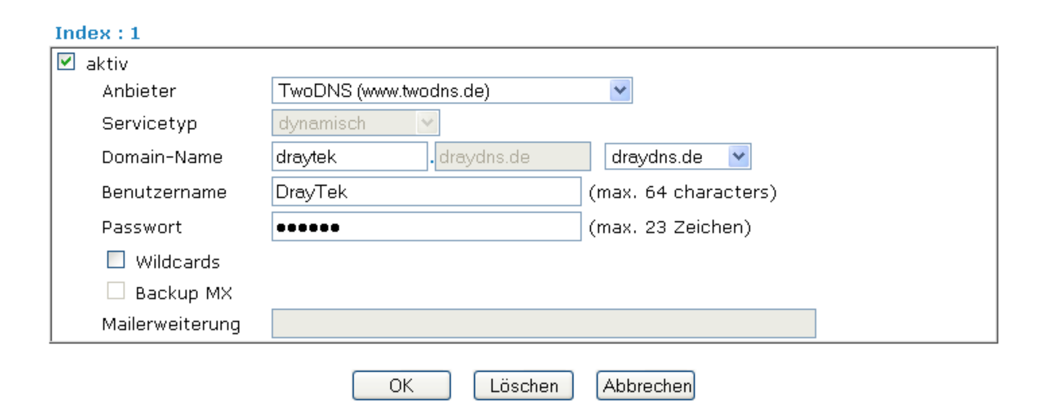
2. Markieren Sie im DDNS-Konfigurationsmenü den Punkt **Aktiv**.



Auf Werkseinstellungen zurücksetzen	Alle Profile löschen und Werkseinstellungen wiederherstellen.
Aktiv	Markieren Sie dieses Kästchen, um die DDNS-Funktion zu aktivieren.
Index	Klicken Sie auf eine Nummer unter Index, um auf die DDNS-Konfigurationsseite zu gelangen.
Domain-Name	Domain-Namen anzeigen, den Sie auf der Seite mit den DDNS-Einstellungen eingegeben haben.
Aktiv	Anzeigen, ob dieses Konto aktiv oder inaktiv ist.
Log ansehen	DDNS-Log-Status anzeigen.
Aktualisieren	Zwingt den Router, seine Information mit dem DDNS-Server zu aktualisieren.

3. Wählen Sie Indexnummer 1, um ein Konto für den Router hinzuzufügen. Markieren Sie **Aktiv**, wählen Sie dyndns.org als Anbieter und geben Sie den registrierten Hostnamen *hostname* und den Domain-Namenssuffix dyndns.org unter **Domain-Name** ein. In den folgenden Feldern geben Sie Ihren Benutzernamen und das Passwort ein.

Anwendungen >> DynDNS >> Konto-Einstellungen



Aktiv	Markieren Sie dieses Kästchen, um das aktuelle Konto zu aktivieren. Wenn Sie dieses Kästchen aktiviert haben, erscheint in der Spalte "Aktiv" auf der vorherigen Web-Seite von Schritt 2. ein Häkchen.
WAN-Schnittstelle	Wählen Sie die WAN-Schnittstelle, auf welcher die Einstellungen angewendet werden sollen.
Anbieter	Wählen Sie den Anbieter für das DDNS-Konto
Servicetyp	Wählen Sie einen Servicetyp (dynamisch, benutzerdefiniert oder statisch). Falls Sie "benutzerdefiniert" wählen, können Sie die Domain ändern, die im Feld "Domain-Name" gewählt ist.
Domain-Name	Geben Sie einen Domain-Namen ein, den Sie zuvor konfiguriert haben. Verwenden Sie die Dropdown-Liste, um die gewünschte Domain zu wählen.
Benutzername	Geben Sie den Benutzernamen ein, den Sie für die Domain konfiguriert haben.

Passwort Geben Sie das Passwort ein, das Sie für die Domain gesetzt haben.

4. Klicken Sie auf **OK**, um die Einstellungen zu aktivieren. Ihre Einstellungen werden gespeichert.

Die Wildcard- und Backup MX-Funktionen werden nicht von allen DDNS-Anbietern unterstützt. Weitere Informationen sind auf den entsprechenden Web-Sites der Anbieter verfügbar.

Funktion deaktivieren und alle dynamischen DNS-Konten löschen

Entfernen Sie im DDNS-Konfigurationsmenü die Markierung von **Aktiv** und klicken Sie auf **Alle löschen**, um die Funktion zu deaktivieren und alle Konten vom Router zu löschen.

Ein dynamisches DNS-Konto löschen

Klicken Sie im DDNS-Konfigurationsmenü auf die **Index**nummer, die Sie löschen möchten, und klicken Sie auf **Löschen**, um das Konto zu löschen.

3.4.2 UPnP

Das **UPnP**-Protokoll (Universal Plug and Play) wird unterstützt, um die Installation und Konfiguration von Netzwerkgeräten zu vereinfachen, wie dies bereits bei direkt angeschlossenen PC-Peripheriegeräten mit dem Windows "Plug and Play"-System der Fall ist. Bei NAT-Routern ist "NAT-Traversal" die wichtigste UPnP-Funktion des Routers. Sie ermöglicht Anwendungen hinter der Firewall, automatisch die Ports zu öffnen, die für die Weiterleitung durch einen Router erforderlich sind. Dies ist verlässlicher, als den Router selbst feststellen zu lassen, welche Ports geöffnet werden müssen. Außerdem muss der Benutzer keine Port-Zuordnungen oder DMZ manuell einrichten. **UPnP ist für Windows XP verfügbar**, und der Router bietet die entsprechende Unterstützung für MSN Messenger, um die Verwendung der Sprach-, Video- und Messaging-Funktionen uneingeschränkt zu ermöglichen.

Anwendungen >> UPnP

UPnP

☑ aktiv

☐ Dienst für die Verbindungskontrolle aktivieren

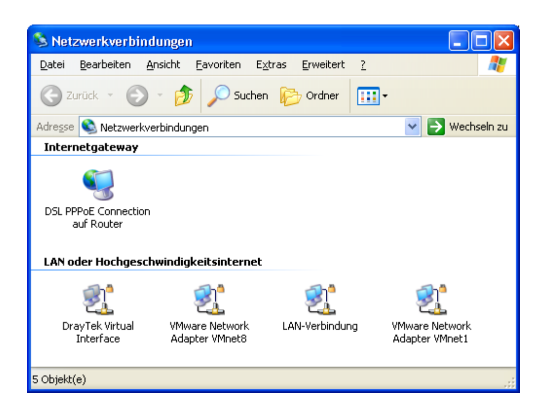
☐ Dienst für den Verbindungsstatus aktivieren

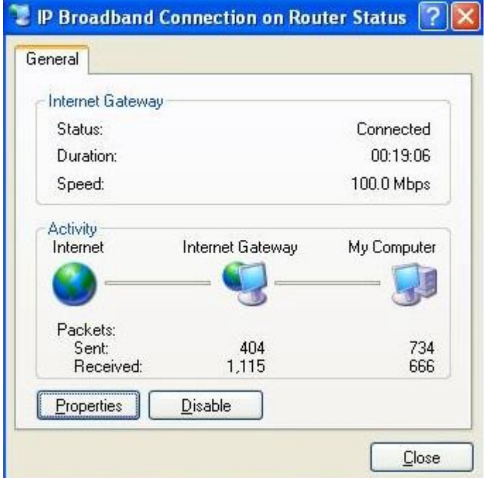
Hinweis: Bei aktivem UPnP kann der Router aus dem LAN heraus veranlasst werden, verschiedene Ports zu öffnen. Es könnten Sicherheitslücken in den NAT- und Firewall-Einstellungen entstehen, weshalb UPnP nur mit Bedacht aktiviert werden sollte.

OK | Löschen | Abbrechen

Aktiv Sie können entweder den Dienst für die **Verbindungskontrolle** oder den Dienst für den **Verbindungsstatus** aktivieren.

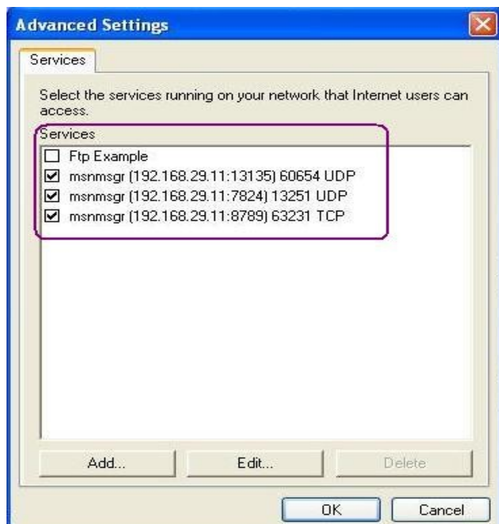
Nachdem diese Funktion auf **Aktiv** gesetzt wurde, erscheint unter Windows XP/Netzwerkverbindungen das Symbol **IP-Breitbandverbindung auf Router**. Der Verbindungsstatus und der Verbindungskontrollstatus können aktiviert werden. Die NAT-Traversal-Funktion von UPnP ermöglicht die Verwendung der Multimedia-Funktionen Ihrer Anwendungen. Die Port-Zuordnungen müssen manuell oder anderweitig eingestellt werden. Die folgenden Screenshots zeigen anhand von Beispielen, wie dies funktioniert.





Die UPnP-Funktion des Routers ermöglicht Anwendungen mit UPnP-Unterstützung wie MSN Messenger, zu erkennen, was sich hinter einem NAT-Router befindet. Die Anwendung erkennt auch die externe IP-Adresse und konfiguriert die Port-Zuordnungen auf dem Router. Danach ermöglicht diese Funktion die Weiterleitung von Paketen von den externen Ports des Routers zu den internen Ports, die von der Anwendung verwendet werden.





Hinweis zur Firewall und UPnP

Probleme mit Firewall-Software
Der Einsatz von Firewall-Anwendungen auf Ihrem Rechner kann die UPnP-Funktion behindern. Dies liegt daran, dass diese Anwendungen den Zugriff auf einige Netzwerk-Ports blockieren.

Sicherheitsüberlegungen
Die Verwendung der UPnP-Funktion in Ihrem Netzwerk kann gewisse Sicherheitsrisiken mit sich bringen. Sie sollten diese Risiken genau abwägen, bevor Sie die UPnP-Funktion aktivieren.

➢ Da die Schwächen der UPnP-Funktion bei manchen Microsoft-Betriebssystemen ausgenutzt werden können, ist es wichtig, die neuesten Service Packs und Patches einzuspielen.

➢ Nicht privilegierte Benutzer können gewisse Router-Funktionen steuern, z.B. Port-Zuordnungen entfernen und hinzufügen.

Die UPnP-Funktion fügt dynamisch Port-Zuordnungen für einige Anwendungen mit UPnP-Unterstützung hinzu. Falls diese Anwendungen abstürzen, kann es sein, dass diese Zuordnungen nicht entfernt werden.

3.5 Wireless LAN

Diese Funktion wird für "n/Vn"-Modelle verwendet.

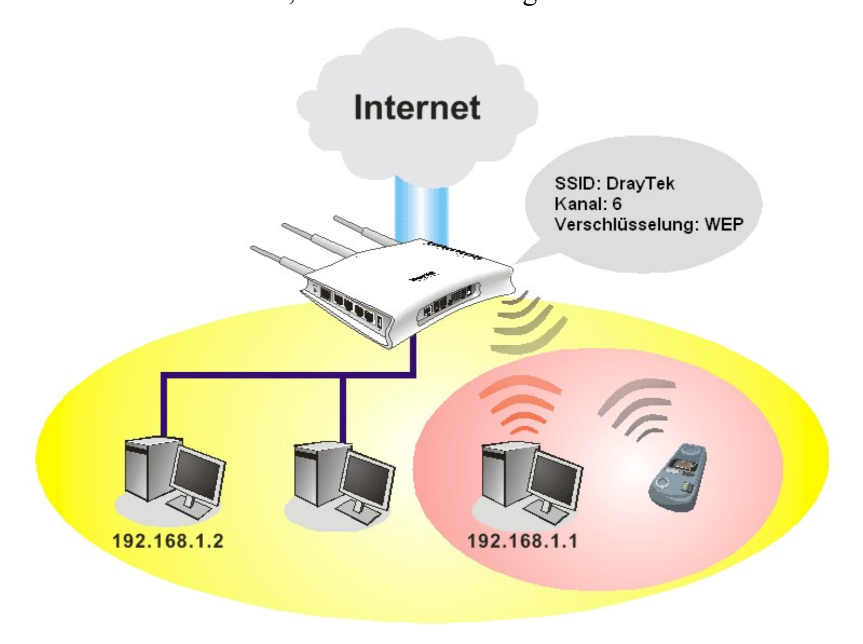
3.5.1 Grundlagen

In den letzten Jahren ist der Markt für kabellose Kommunikation enorm gewachsen. Praktisch jeder Punkt auf der Erde wird mit Wireless-Technologie erreicht oder kann erreicht werden. Viele Menschen tauschen jeden Tag über Wireless-Kommunikationsprodukte Informationen aus. Das Vigor-Modell "n", d.h. der Vigor-Wireless-Router, wurde im Hinblick auf maximale Flexibilität und Effizienz im Kleinunternehmen/Privatbereich konzipiert. Jeder berechtigte Mitarbeiter kann ohne Kabelsalat und Löcher in den Wänden ein WLAN-fähiges PDA oder Notebook im Besprechungszimmer verwenden. Die Mobilität im Wireless LAN ist so hoch entwickelt, dass WLAN-Benutzer gleichzeitig Zugriff auf die gesamte LAN-Ausstattung und auf das Internet haben, genau wie dies bei einem kabelgebundenen LAN der Fall wäre.

Vigor-Wireless-Router sind mit einer WLAN-Schnittstelle ausgerüstet, die dem Standard IEEE 802.11n entspricht. Die fortgeschrittene Wireless-Technologie des Vigor-Routers sorgt für eine weitere Leistungssteigerung, die Übertragungsgeschwindigkeiten von bis zu 300 Mbps* ermöglicht. Endlich können Sie nun ruckelfreie Audio- und Videoübertragungen genießen!

Hinweis: * Der tatsächliche Datendurchsatz ändert sich je nach Netzwerkbedingungen und Faktoren wie dem Netzwerkverkehrsvolumen, dem Netzwerk-Overhead und den Objekten in der Umgebung.

In einem Wireless-Netzwerkinfrastrukturmodus dient der Vigor-Wireless-Router als Access Point (AP), mit dem sich verschiedene WLAN-Clients bzw. Stationen (STA) verbinden können. Alle STAs teilen sich den gleichen Internetanschluss über den Wireless-Router. Unter **Basiskonfiguration** werden die Daten zu diesem Wireless-Netzwerk wie die SSID, der Kanal usw. eingestellt.



Verschlüsselungsfunktionen

Echtzeit-Hardware-Verschlüsselung: Der Vigor-Router ist mit einer Hardware-AES-Verschlüsselungs-Engine ausgestattet, um maximalen Schutz der Daten ohne Beeinträchtigung der Nutzung zu ermöglichen.

Umfassende Auswahl von Verschlüsselungsnormen: Um die Sicherheit und die Vertraulichkeit Ihrer Wireless-Kommunikation zu sichern, bieten wir verschiedene marktübliche Normen an.

WEP (Wired Equivalent Privacy) ist eine ältere Methode zur Verschlüsselung jedes per Funk übertragenen Datenpakets mit einem 64- oder 128-Bit-Schlüssel. Normalerweise gibt der Access Point vier Schlüssel vor, wobei nur einer für die Kommunikation mit den einzelnen Clients verwendet wird.

WPA (Wi-Fi Protected Access), der vorherrschende Sicherheitsmechanismus in diesem Sektor, umfasst zwei Kategorien: WPA-Personal, auch bekannt als WPA Pre-Shared Key (WPA/PSK), und WPA-Enterprise, auch bekannt als WPA/802.1x.

Bei WPA-Personal wird während der Datenübertragung ein Pre-Shared Key (vorher vereinbarter Schlüssel) für die Verschlüsselung verwendet. WPA benutzt für die Datenverschlüsselung Temporal Key Integrity Protocol (TKIP), und WPA2 verwendet AES. WPA-Enterprise wird nicht nur für die Verschlüsselung, sondern auch für die Authentifizierung benutzt.

Da sich herausgestellt hat, dass WEP verletzlich ist, ist WPA als sicherste Verbindung zu empfehlen. Wählen Sie Ihren Bedürfnissen entsprechend den geeignetsten Sicherheitsmechanismus. Letztendlich verbessert jede Sicherheitsfunktion den Schutz Ihrer Funkdaten und/oder die Privatsphäre Ihres Wireless-Netzwerks. Der Wireless-Router von Vigor ist sehr flexibel und unterstützt gleichzeitig mehrere sichere Verbindungen mit WEP und WPA.

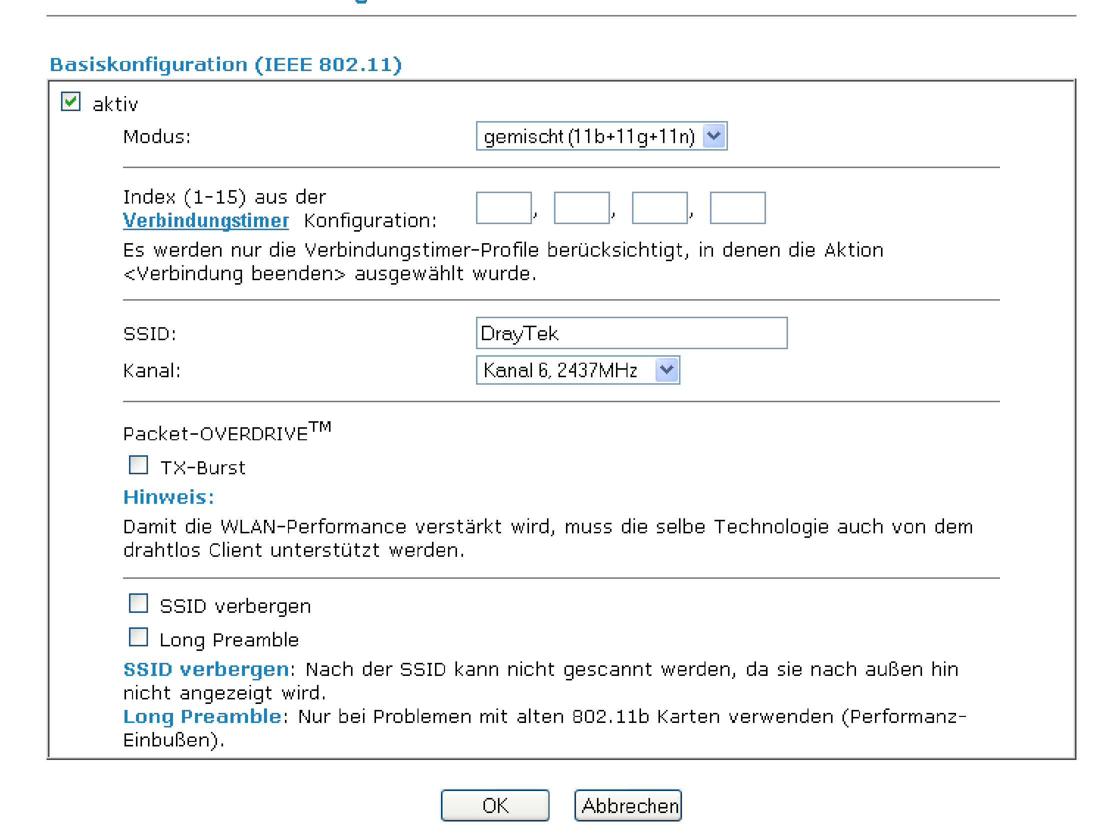
Die **Trennung des Wireless LAN vom kabelgebundenen LAN (WLAN-Isolation)** ermöglicht Ihnen, Ihr Wireless LAN für Quarantäne- oder Zugriffsbeschränkungszwecke vom kabelgebundenen LAN zu isolieren. "Isolieren" bedeutet in diesem Zusammenhang, dass die Parteien keinen Zugriff aufeinander haben. Im geschäftlichen Bereich kann beispielsweise ein Wireless LAN speziell für Besucher eingerichtet werden, so dass diese Zugang zum Internet haben, ohne jedoch auf vertrauliche Daten zugreifen zu können. Weitere Flexibilität kann dadurch erreicht werden, dass MAC-Adressfilter eingesetzt werden, um den Zugriff von Benutzern des kabelgebundenen LANs zu isolieren.

Die **Verwaltung der Wireless-Clients (Liste der Clients)** führt alle Clients in Ihrem Wireless-Netzwerk und ihren Verbindungsstatus auf.

Die folgende Abbildung zeigt die Menüeinträge für Wireless LAN an:



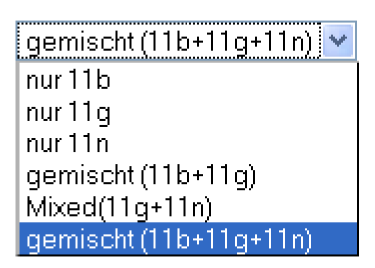
3.5.2 Basiskonfiguration



Wenn Sie auf **Basiskonfiguration** klicken, erscheint eine neue Web-Seite, auf der Sie die SSID und den Wireless-Kanal einstellen können. Die folgende Abbildung enthält weitere Informationen:

Aktiv Markieren Sie dieses Kästchen, um die Wireless-Funktion zu aktivieren.

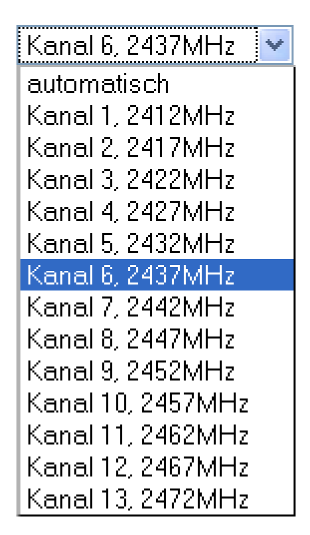
Modus Zur Zeit kann sich der Router über die Modi Gemischt (11b+11g), Nur 11g, Nur 11b, Gemischt (11g+11n), Nur 11n und Gemischt (11b+11g+11n) mit Clients verbinden. Wählen Sie einfach den Modus Gemischt (11b+11g+11n).



Index (1-15) Sie können das Wireless LAN so konfigurieren, dass es lediglich in gewissen Zeitabschnitten in Betrieb ist. Sie können bis zu vier der 15 vordefinierten Timer unter **Anwendungen** >> **Timer** wählen. Per Standardeinstellung ist dieses Feld leer, und die Funktion ist ständig in Betrieb.

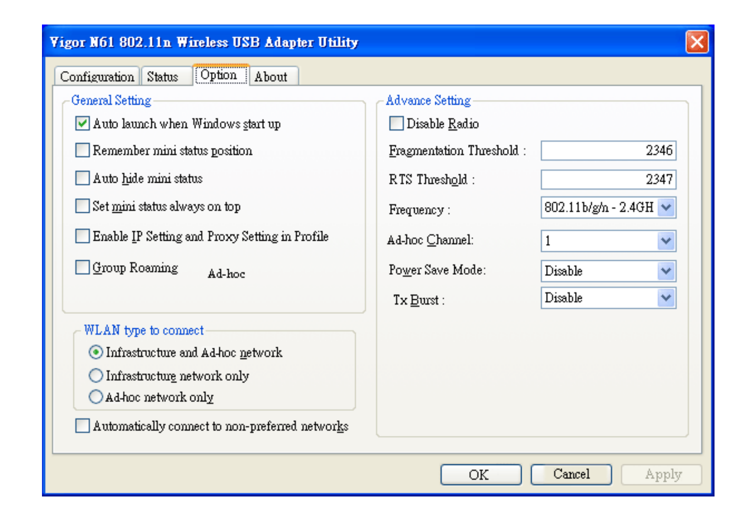
SSID Dies ist die Bezeichnung des Wireless LANs. Die SSID kann aus alphanumerischen Zeichen und Sonderzeichen bestehen. Die Standard-SSID ist "DrayTek". Wir empfehlen, diese zu ändern.

Kanal Gibt den Frequenzkanal des Wireless LANs an. Der Standardkanal ist 6. Ändern Sie den gewählten Kanal, falls dieser starken Funkstörungen ausgesetzt ist. Falls Sie nicht wissen, welche Frequenz geeignet ist, wählen Sie Auto, um das System die Auswahl treffen zu lassen.



Packet-OVERDRIVE Diese Funktion kann die Datenübertragungsleistung um ca. 40%* verbessern (durch Markieren von **Tx-Burst**). Es ist aktiv, wenn sowohl der Access Point als auch die Station (im Wireless-Client) die Funktion gleichzeitig verwendet. Dies bedeutet, dass der Wireless-Client diese Funktion sowohl unterstützen als auch aktivieren muss.

Hinweis: Der Vigor N61 Wireless Adapter unterstützt diese Funktion. Sie können diesen verwenden und in Ihrem Rechner installieren, um die Nutzung von Packet-OVERDRIVE zu ermöglichen (sehen Sie das folgende Bild des Vigor N61 Wireless Konfigurationsfensters; hier muss im Fenster **Optionen** die Funktion **TxBURST** auf **Aktiv** gesetzt werden).



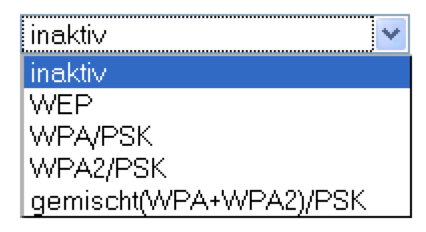
SSID verbergen	Markieren Sie dieses Kästchen, um Wireless-Sniffing zu vermeiden und es für unbefugte Clients oder STAs schwieriger zu machen, sich an Ihrem Wireless LAN anzumelden. Je nach verwendeter Wireless-Technik kann der Benutzer bei der Netzwerksuche lediglich die Information ohne SSID oder überhaupt nichts über den Vigor-Wireless-Router sehen. Das System erlaubt die Eingabe von vier verschiedenen SSIDs für unterschiedliche Zwecke. Standardmäßig wird die erste SSID aktiviert. Sie können diese bei Bedarf verbergen.
Long Preamble	Diese Option dient der Bestimmung der Länge des Sync-Feldes in einem 802.11-Paket. Die meisten modernen Wireless-Netzwerke verwenden kurze Präambeln mit 56-Bit Sync-Feld anstatt der langen Präambel mit 128-Bit Sync-Feld. Manche originäre 11b Wireless-Netzwerkgeräte unterstützen jedoch nur lange Präambeln. Markieren Sie **Long Preamble**, falls dies erforderlich ist, um mit dieser Art von Geräten zu kommunizieren.

3.5.3 Verschlüsselung

Wenn Sie auf **Verschlüsselung** klicken, erscheint eine neue Web-Seite, auf der Sie die WEP- und WPA-Einstellungen konfigurieren können.

Modus

Es stehen verschiedene Modi zur Auswahl.



Inaktiv - Verschlüsselung abschalten.

WEP - Akzeptiert nur WEP-Clients; der Schlüssel für die Verschlüsselung muss unter WEP-Schlüssel eingetragen werden.

WPA/PSK - Akzeptiert nur WPA-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingeben werden.

WPA2/PSK -Akzeptiert nur WPA2-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingegeben werden.

Gemischt (WPA+ WPA2)/PSK - Akzeptiert gleichzeitig WPA- und WPA2-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingegeben werden.

WPA

WPA verschlüsselt jedes per Funk übertragene Paket entweder mit dem PSK (Pre-Shared Key), der in dem Feld unten manuell eingegeben wurde, oder mit dem automatisch per 802.1x-Authentifizierung verhandelten Schlüssel. Hierzu werden entweder **8~63** ASCII-Zeichen, z.B. "012345678..." oder 64 hexadezimale Ziffern, angeführt von "0x", z.B. "0x321253abcde..." verwendet.

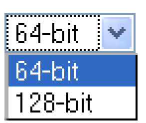
Typ - Auswahl zwischen Gemischt (WPA+WPA2) oder Nur WPA2.

Pre-Shared Key (PSK) - Entweder **8~63** ASCII-Zeichen, z.B. "012345678..." oder 64 hexadezimale Zeichen, angeführt von "0x", z.B. "0x321253abcde...".

WEP

64-Bit - Für 64-Bit WEP-Schlüssel; entweder **5** ASCII-Zeichen, z.B. "12345", oder 10 hexadezimale Ziffern, angeführt von "0x", z.B. "0x4142434445".

128-Bit - Für 128-Bit WEP-Schlüssel; entweder **13** ASCII-Zeichen, z.B. "ABCDEFGHIJKLM", oder 26 hexadezimale Ziffern, angeführt von "0x", z.B. "0x4142434445464748494A4B4C4D".



Alle Wireless-Geräte müssen die gleiche WEP-Verschlüsselungslänge unterstützen und den gleichen Schlüssel verwenden. Hier können **vier Schlüssel** eingegeben werden, aber es kann jeweils nur ein Schlüssel ausgewählt werden. Die Schlüssel können in ASCII oder hexadezimal eingegeben werden. Haken Sie den Schlüssel an, den Sie verwenden möchten.

3.5.4 Zugriffskontrolle

Um den Wireless-Zugriff zusätzlich abzusichern, ermöglicht Ihnen die **Zugriffskontrolle**, den Zugriff auf das Netzwerk über die Wireless LAN MAC-Adresse des Clients zu steuern. So wird nur gültigen MAC-Adressen erlaubt, auf die Wireless LAN Schnittstelle zuzugreifen. Wenn Sie auf **Zugriffskontrolle** klicken, erscheint eine neue Web-Seite wie unten abgebildet, in der Sie die MAC-Adressen der Clients bearbeiten können, um deren Zugriffsrechte zu steuern.

Wireless LAN >> Zugriffskontrolle

Zugriffskontrolle

aktiv

Modus: Weisse MAC-Adressen Liste

MAC-Adressen Filter

Index Attribut MAC-Adresse

Client MAC-Adresse : : : : : :

Attribut :

s: Client vom LAN isolieren

Hinzufügen Löschen Bearbeiten Abbrechen

OK Alles löschen

Aktiv	Markieren Sie dieses Kästchen, um die Zugriffskontrolle über die MAC-Adresse zu aktivieren.
Modus	Wählen Sie einen der folgenden Modi. Markieren Sie **MAC-Whitelist**, um die MAC-Adressen für andere Clients im Netzwerk manuell einzugeben. Wenn Sie **WLAN vom LAN isolieren** wählen, werden alle WLAN-Clients auf der Grundlage der MAC-Adressenliste vom LAN getrennt.
MAC-Adressenfilter	Alle MAC-Adressen anzeigen, die zuvor bearbeitet wurden.
	MAC-Adresse des Clients - Geben Sie die MAC-Adresse des Wireless-Clients manuell ein.
Attribut	**s: Client vom LAN isolieren -** Markieren, um die Wireless-Verbindung des Wireless-Clients mit der MAC-Adresse vom LAN zu trennen.
Hinzufügen	Der Liste eine neue MAC-Adresse hinzufügen.
Löschen	Ausgewählte MAC-Adresse aus der Liste löschen.
Bearbeiten	Ausgewählte MAC-Adresse in der Liste bearbeiten.
Abbrechen	Konfiguration der Zugriffskontrolle abbrechen.
OK	ACL speichern.
Alle löschen	Alle Einträge in der MAC-Adressenliste löschen.

3.5.5 Liste der Clients

Die **Liste der Clients** enthält Informationen über die aktuell verbundenen Clients und den Status-Code. Die Codes werden unten erläutert. Zwecks **Zugriffskontrolle** können Sie einen WLAN-Client wählen und auf **Hinzufügen** klicken.

Wireless LAN >> Liste der Clients

Liste der Clients

Status MAC-Adresse verbunden mit

Aktualisieren

Statusdefinitionen :
C: verbunden, keine Verschlüsselung
E: verbunden, WEP
P: verbunden, WPA
A: verbunden, WPA2
B: blockiert durch die Zugriffskontrolle
N: Verbindungsaufbau
F: WPA/PSK Authentifizierung fehlgeschlagen

Hinweis: Ist die WLAN-Verbindung zwischen dem Router und einem Client unterbrochen, wird der WLAN-Client aufgrund von Verzögerungen nicht sofort aus der Liste entfernt.

Hinzufügen zur Zugriffskontrolle :

MAC-Adresse des Clients : : : : :

Hinzufügen

Aktualisieren	Klicken Sie auf diese Taste, um den Status der Client-Liste zu aktualisieren.
Hinzufügen	Klicken Sie auf diese Taste, um die eingegebene MAC-Adresse der **Zugriffskontrolle** hinzuzufügen.

3.6 Systemmanagement

Es gibt verschiedene Bereiche, die für die Konfiguration von Bedeutung sind: Status, Administratorpasswort, Konfigurations-Backup, Syslog, Zeit und Datum, Neustart und Aktualisierung der Firmware.

Die folgende Abbildung zeigt die Menüeinträge für das Systemmanagement:



3.6.1 Systemstatus

Im **Systemstatus** sehen Sie grundlegende Netzwerkeinstellungen des Vigor-Routers. Dies umfasst Informationen über die LAN- und WAN-Schnittstellen. Außerdem werden die aktuelle Version und Informationen bezüglich dieser Firmware angezeigt.

Systemstatus

Modellname	: Vigor2710 series
Firmwareversion	: 3.2.3_2111112
Erstellungsdatum	: Feb 12 2009 18:35:57
ADSL-Modemcode	: 2111112_B Annex A

LAN	
MAC-Adresse	: 00-50-7F-8F-FA-B8
NAT IP-Adresse	: 192.168.1.1
NAT Subnetz-Maske	: 255.255.255.0
DHCP-Server	: Ja
DNS	: 194.109.6.66

WAN	
Verbindungsstatus	: getrennt
MAC-Adresse	: 00-50-7F-8F-FA-B9
Verbindung	: PPPoE
IP-Adresse	: ---
Standard-Gateway	: ---

Port	Profil	Reg.	Rein/Raus
Phone1		Nein	0/0
FXS2		Nein	0/0

Wireless LAN	
MAC-Adresse	: 00-50-7f-8f-fa-b8
Frequenzbereich	: Europe
Firmwareversion	: 1.8.1.0
SSID	: DrayTek

Modellname	Modellname des Routers
Firmwareversion	Firmwareversion des Routers
Erstellungsdatum	Datum und Uhrzeit der Erstellung der aktuellen Firmware
ADSL-Modemcode	ADSL-Firmwareversion
LAN-------	
MAC-Adresse	MAC-Adresse der LAN-Schnittstelle
NAT IP-Adresse	IP-Adresse der LAN-Schnittstelle
Subnetz-Maske	Adresse der Subnetz-Maske der LAN-Schnittstelle
DHCP-Server	Aktueller Status des DHCP-Servers der LAN-Schnittstelle
DNS	Zugewiesene IP-Adresse des bevorzugten DNS-Servers
WAN-------	
Verbindungsstatus	Aktueller Verbindungsstatus
MAC-Adresse	MAC-Adresse der WAN-Schnittstelle
Verbindung	Verbindungsart
IP-Adresse	IP-Adresse der WAN-Schnittstelle

Standard-Gateway Zugewiesene IP-Adresse des Standard-Gateways

Wireless LAN-------

MAC-Adresse MAC-Adresse des Wireless LANs

Frequenzbereich Zur Auswahl stehen Europa (13 verwendbare Kanäle), USA (11 verwendbare Kanäle), usw. Die von Wireless-Geräten unterstützten Kanäle unterscheiden sich von Land zu Land.

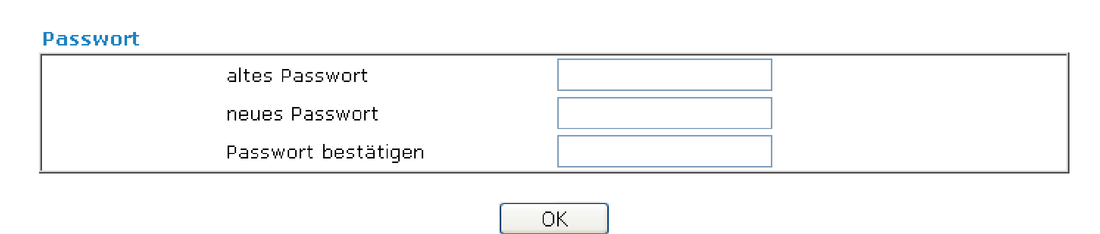
Firmwareversion Zeigt Informationen zur WLAN Mini-PCI-Karte an. Daraus ergibt sich die Verfügbarkeit einiger Funktionen, die mit der WLAN Mini-PCI-Karte zusammenhängen.

SSID SSID des Routers

3.6.2 Benutzerpasswort

Auf dieser Seite können Sie ein neues Passwort für den Benutzermodus setzen.

Systemmanagement >> Passwort



Altes Passwort Geben Sie das alte Passwort ein. Per Werkseinstellung ist das Passwort leer.

Neues Passwort Geben Sie das neue Passwort in diesem Feld ein.

Passwort bestätigen Geben Sie das neue Passwort erneut ein.

Wenn Sie auf OK klicken, erscheint das Anmeldefenster. Bitte benutzen Sie das neue Passwort, um sich erneut im Router-Menü anzumelden.

3.6.3 Zeit und Datum

Hier können Sie angeben, wo der Router die Uhrzeit abfragen soll.

Systemmanagement >> Zeit und Datum

Zeitinformation

Aktuelle Systemzeit 2009 Jul 7 Tue 15 : 51 : 36 Zeit abrufen

Zeit und Datum

Rechner/Browser-Zeit

Internet-Zeit

Server-IP pool.ntp.org

Zeitzone (GMT+01:00) Amsterdam, Berlin, Bern

autom. auf Sommer-/Winterzeit umstellen

Aktualisierungsintervall 5 Stunden

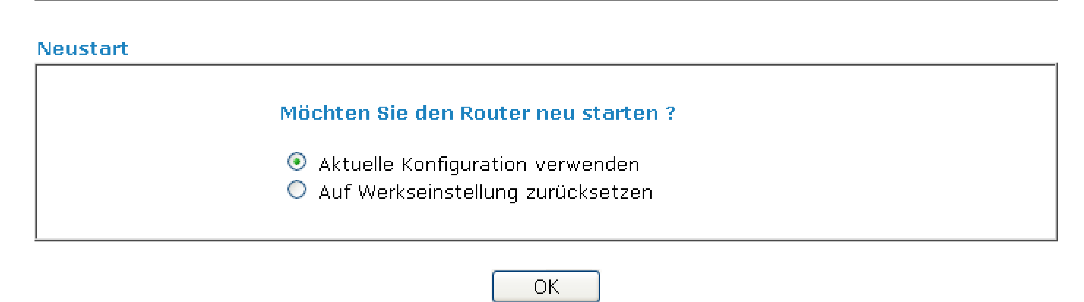
OK Abbrechen

Aktuelle Systemzeit	Klicken Sie auf **Zeit abrufen**, um die aktuelle Zeit zu erhalten.
Rechner-/Browserzeit	Wählen Sie diese Option, um die Browser-Zeit des entfernten Rechners des Administrators als Systemzeit für den Router zu verwenden.
Internet-Zeit	Wählen Sie diese Option, um die Zeit über das gewählte Protokoll von Zeitservern im Internet abzufragen.
Zeitprotokoll	Auswahl des Zeitprotokolls.
Server-IP	IP-Adresse des Zeitservers eingeben.
Zeitzone	Zeitzone auswählen, in der sich der Router befindet.
Autom. auf Sommer-/Winterzeit umstellen	Markieren Sie dieses Kästchen, um automatisch auf Sommer-/Winterzeit umzustellen. Diese Funktion ist in einigen Regionen sinnvoll.
Aktualisierungsintervall	Wählen Sie ein Zeitintervall für die Aktualisierung vom NTP-Server.

Klicken Sie auf **OK**, um diese Einstellungen zu speichern.

3.6.4 Neustart

Der Router kann aus dem Konfigurationsmenü heraus neu gestartet werden, um die aktuelle Konfiguration anzuwenden. Wählen Sie **Neustart** unter **Systemmanagement**, um die folgende Seite zu öffnen:



Klicken Sie auf **OK**. Der Router benötigt fünf Sekunden, um das System neu zu starten.

> **Hinweis:** Wenn das System nach Konfiguration der Internet-Einstellungen die Web-Seite für den Neustart des Systems anzeigt, klicken Sie bitte auf **OK**, um Ihren Router neu zu starten und so den ordnungsgemäßen Betrieb sicherzustellen und unerwartete Router-Probleme in der Zukunft zu vermeiden.

3.7 Diagnose-Tools

Die Diagnose-Tools eignen sich zur **Kontrolle** oder **Diagnose** des Status Ihres Vigor-Routers.

Die folgende Abbildung zeigt die Menüeinträge für die Diagnose-Tools:

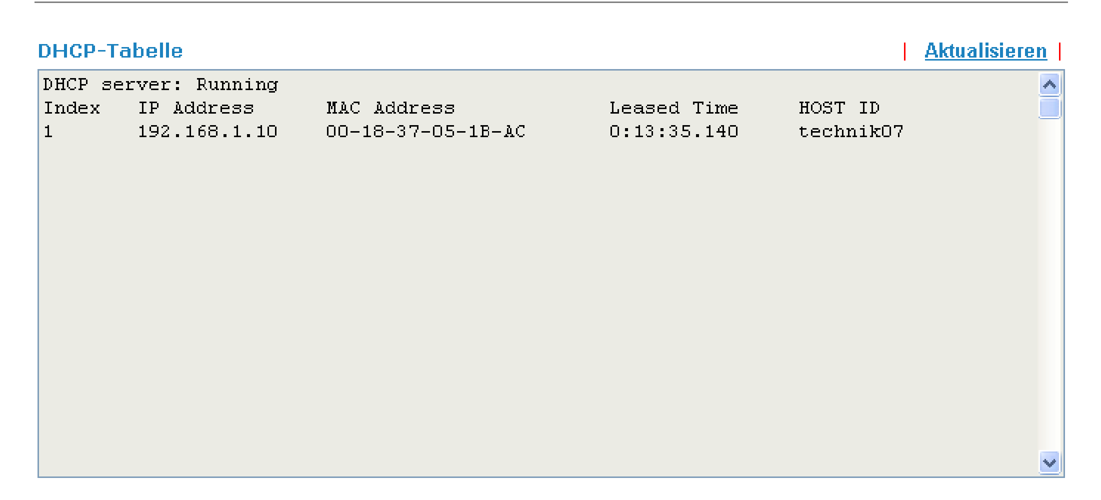


3.7.1 DHCP-Tabelle

Diese Tabelle liefert Informationen zur Zuweisung von IP-Adressen. Diese Informationen sind nützlich für die Diagnose von Netzwerkproblemen wie IP-Adressenkonflikte usw.

Wählen Sie **Diagnose-Tools** und klicken auf **DHCP-Tabelle**, um die Web-Seite zu öffnen.

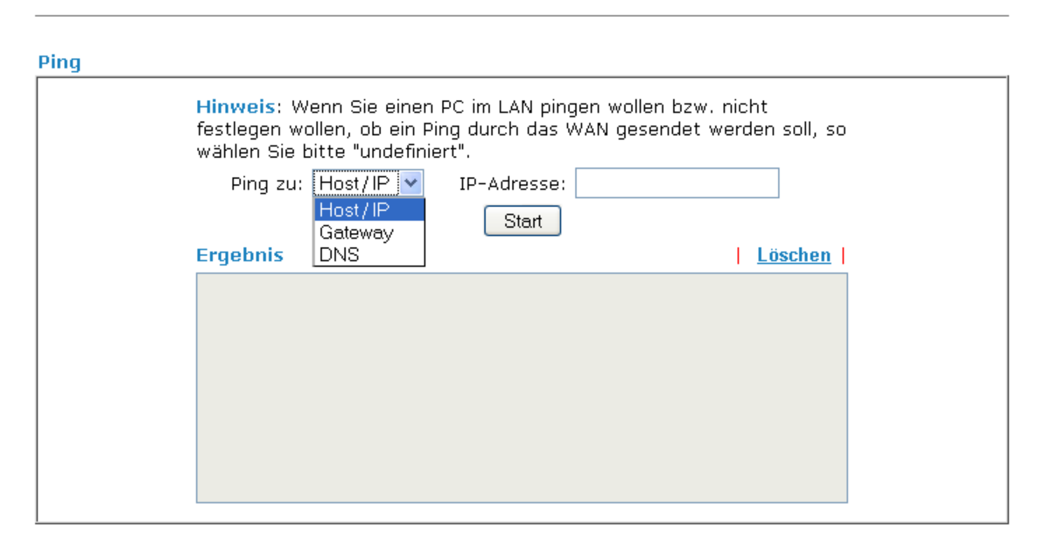
Diagnose-Tools >> DHCP-Tabelle



Index	Zeigt die Verbindungsnummer an.
IP-Adresse	Zeigt die IP-Adresse an, die dieser Router dem angegebenen Rechner zugewiesen hat.
MAC-Adresse	Zeigt die MAC-Adresse des angegebenen Rechners an, der DHCP eine IP-Adresse zugewiesen hat.
Lease Time	Zeigt die Lease Time des angegebenen Rechners an.
Host-ID	Zeigt die Host-ID des angegebenen Rechners an.
Aktualisieren	Anklicken, um die Seite neu zu laden.

3.7.2 Ping

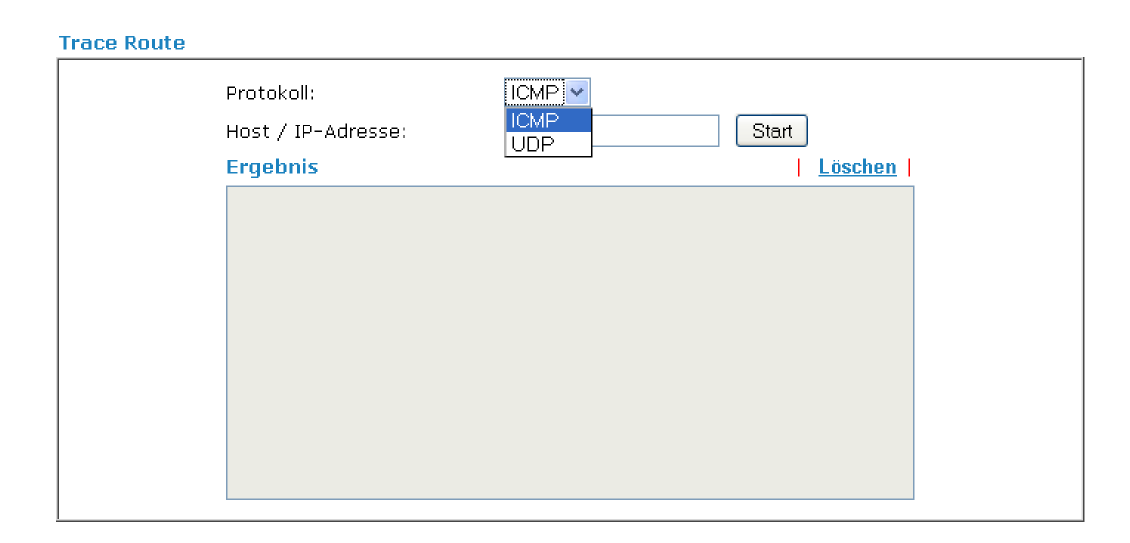
Wählen Sie **Diagnose-Tools** und klicken auf **Ping**, um die Web-Seite zu öffnen.



Ping zu	Verwenden Sie die Dropdown-Liste, um das Ziel zu wählen, das Sie anpingen möchten.
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, den Sie anpingen möchten.
Start	Klicken Sie auf diese Schaltfläche, um Ping zu starten. Das Ergebnis wird auf dem Bildschirm angezeigt.
Löschen	Klicken Sie auf diesen Link, um die Ausgabe im Fenster zu löschen.

3.7.3 Trace Route

Wählen Sie **Diagnose-Tools** und klicken auf **Trace Route**, um die Web-Seite zu öffnen. Auf dieser Seite können Sie den Pfad vom Router zum Host nachverfolgen. Geben Sie einfach die IP-Adresse des Hosts im Feld ein und klicken auf **Ausführen**. Das Ergebnis wird auf dem Bildschirm angezeigt.



Protokoll	Verwenden Sie die Dropdown-Liste, um die Schnittstelle zu wählen, durch die Sie pingen möchten.
Host/IP-Adresse	Zeigt die Host-IP-Adresse an.
Start	Klicken Sie auf diese Taste, um Trace Route zu starten.
Löschen	Klicken Sie auf diesen Link, um die Ausgabe im Fenster zu löschen.



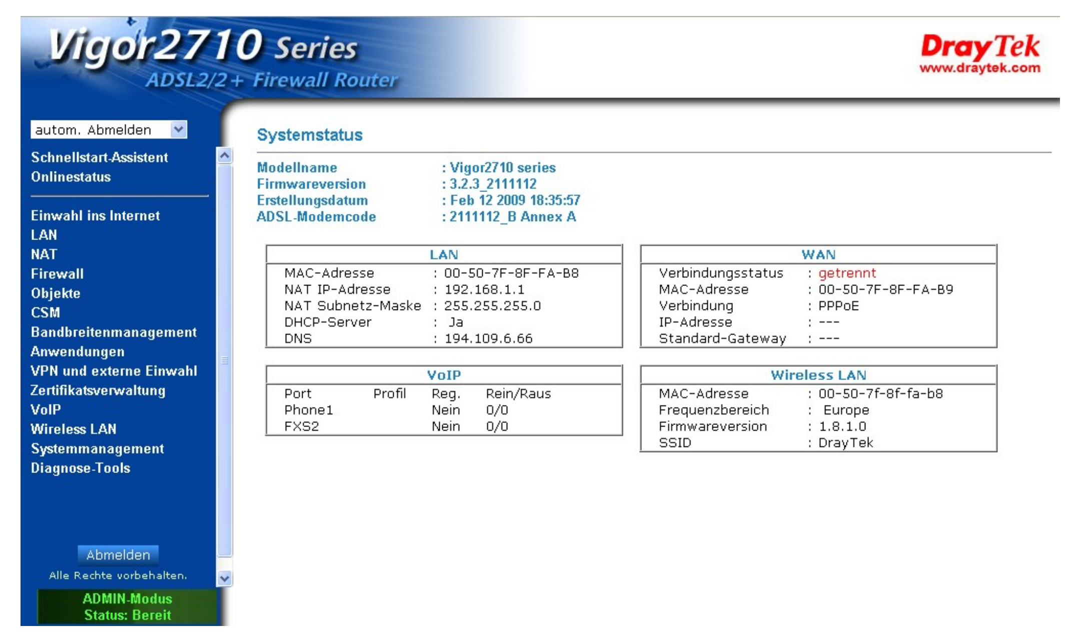
Administratormodus

Dieses Kapitel führt Benutzer durch die erweiterte (volle) Konfiguration im Administratormodus. Weitere Anwendungsfälle werden in Kapitel 5 beschrieben.

3. Starten Sie auf Ihrem PC einen Web-Browser und geben Sie **http://192.168.1.1** ein. Das folgende Fenster erscheint und fragt den Benutzernamen und das Passwort ab.

4. Für den Administratormodus geben Sie unter Benutzername/Passwort "admin/admin" ein.

Das **Hauptfenster** erscheint. Unten links wird "ADMIN-Modus" angezeigt.



4.1 Einwahl ins Internet

Der **Schnellstart-Assistent** bietet Benutzern eine einfache Möglichkeit, den Verbindungsmodus für den Router schnell einzurichten. Falls Sie weitere Einstellungen für verschiedene WAN-Modi konfigurieren möchten, gehen Sie bitte ins Menü **WAN** und klicken auf **Einwahl ins Internet**.

4.1.1 Grundlagen des Internet Protocol (IP) Netzwerks

IP ist die Abkürzung für Internet Protocol. Jedes Gerät in einem IP-basierten Netzwerk (z.B. Router, Printserver und Host-PCs) benötigt eine IP-Adresse, welche dessen Standort im Netzwerk bestimmt. Um Adressenkonflikte zu vermeiden, sind IP-Adressen öffentlich beim Network Information Center (NIC) registriert. Eine unverwechselbare IP-Adresse ist für Geräte im öffentlichen Netzwerk unbedingt erforderlich, nicht jedoch in den privaten lokalen TCP/IP-Netzwerken (LANs), da auf diese kein öffentlicher Zugriff nötig ist. Dies können beispielsweise Host-PCs sein, die von einem Router verwaltet werden. Aus diesem Grunde hat das NIC gewisse Adressen reserviert, die niemals öffentlich registriert werden. Diese werden als ***private*** IP-Adressen bezeichnet und umfassen die folgenden Bereiche:

Von 10.0.0.0 bis 10.255.255.255
Von 172.16.0.0 bis 172.31.255.255
Von 192.168.0.0 bis 192.168.255.255

Öffentliche IP-Adressen und private IP-Adressen

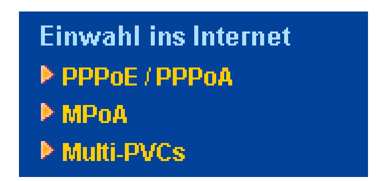
Der Router, der für die Verwaltung und den Schutz seines LANs verantwortlich ist, verbindet Gruppen von Host-PCs. Der eingebaute DHCP-Server des Vigor-Routers weist jedem dieser PCs eine private IP-Adresse zu. Der Router selbst verwendet für die Kommunikation mit den lokalen Hosts standardmäßig die **private IP**-Adresse 192.168.1.1. Zur Kommunikation mit anderen Netzwerkgeräten verwendet der Vigor-Router eine **öffentliche IP**-Adresse. Beim Durchfluss der Daten wandelt die Network Address Translation (NAT) Funktion des Routers öffentliche/private Adressen um, und die Pakete werden dem entsprechenden Host-PC im LAN ausgeliefert. Auf diese Weise können alle Host-PCs einen gemeinsamen Internetanschluss nutzen.

Öffentliche IP-Adresse vom ISP beziehen

Beim Einsatz für ADSL muss für eine erfolgreiche Verbindung von Endgeräten PPP-Authentifizierung und Autorisierung verwendet werden. Point-to-Point Protocol over Ethernet (PPPoE) verbindet ein Netzwerk von Hosts über ein Zugriffsgerät mit einem Fernzugriffskonzentrator. Dieser Ansatz vereinfacht die Nutzung für Benutzer. Je nach Benutzeranforderung ermöglicht dies die Zugriffskontrolle, Abrechnung und Angabe der Dienstart (ToS).

Wenn sich ein Router mit Ihrem ISP verbindet, finden verschiedene Verbindungsprozesse statt, um eine Verbindung anzufordern. Dann wird eine Sitzung aufgebaut. Ihr Benutzername und Ihr Passwort werden über **PAP** oder **CHAP** mit dem **RADIUS**-Authentifizierungssystem authentifiziert. Normalerweise werden die IP-Adresse, die DNS-Server und andere Informationen vom ISP zugewiesen.

Die folgende Abbildung zeigt die Menüeinträge für die Einwahl ins Internet:



4.1.2 PPPoE/PPPoA

PPPoA (beschrieben in RFC1483) kann entweder mit dem LLC-Subnetzwerkzugangsprotokoll oder im VC-Mux-Modus verwendet werden. Als Endgerät kapselt der Vigor-Router die PPP-Sitzung für den Transport über die ADSL-Leitung und die DSL-Vermittlungsstelle (DSLAM) Ihres ISPs.

Um PPPoE oder PPPoA als Zugangsprotokoll für das Internet zu verwenden, wählen Sie **PPPoE/PPPoA** im Menü **Einwahl ins Internet**. Die folgende Web-Seite erscheint:

Einwahl ins Internet >> PPPoE / PPPoA

PPPoE / PPPoA Einstellungen

PPPoE/PPPoA ⦿ aktiv ○ inaktiv

DSL-Modem Einstellungen

Multi-PVC Kanal: Kanal 1
VPI: 0
VCI: 33
Kapselung: LLC/SNAP
Protokoll: PPPoE
Modulation: Multimode

PPPoE-Weiterleitung für

☐ kabelgebundenes LAN
☐ Wireless LAN

ISP-Einstellungen

Name des Anbieters
Benutzername
Passwort
PPP-Authentifizierung: PAP oder CHAP
☑ immer in Betrieb
Max. Leerlaufzeit: -1 Sekunden

IP-Adresse des Anbieters [WAN-IP Alias]

feste IP ○ Ja ⦿ Nein (dynamische IP)
feste IP-Adresse

⦿ Voreingestellte MAC-Adresse verwenden
○ MAC-Adresse selbst definieren
MAC-Adresse: 00 : 50 : 7F : 8F : FA : B9

Index (1-15) aus der Verbindungstimer Konfiguration:
=> , , ,

OK

Aktiv/Inaktiv Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

DSL-Modemeinstellungen Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind unerlässlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.

Multi-PVC-Kanal - Die hier angezeigte Auswahl wird von der Seite **Einwahl ins Internet** – **Multi PVC** bestimmt. **M-PVC-Kanal auswählen** bedeutet, dass keine Auswahl markiert wird.

VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.

Protokoll - Dropdown-Liste zur Auswahl des vom ISP bestimmten Protokolls.

Falls Sie das Protokoll bereits mit dem **Schnellstart-Assistent**en eingestellt haben, brauchen Sie hier keine Einstellungen zu ändern.

PPPoE Pass-Through Der Router bietet die Möglichkeit, eine PPPoE-Wählverbindung einzurichten. Außerdem können Sie die PPPoE-Verbindung über den Vigor-Router direkt von den lokalen Clients zum ISP aufbauen. Falls das PPPoA-Protokoll ausgewählt ist, wird das vom PC übertragene PPPoE-Paket in ein PPPoA-Paket umgewandelt und an den WAN-Server übermittelt. Über diese Weiterleitung kann der PC auf das

Internet zugreifen.

Kabelgebundenes LAN – Falls Sie dieses Kästchen markieren, können PCs im gleichen Netzwerk für den Internetzugang eine andere PPPoE-Sitzung verwenden (anders als ein Host-PC).

Wireless LAN – Falls Sie dieses Kästchen markieren, können PCs im gleichen Wireless-Netzwerk für den Internetzugang eine andere PPPoE-Sitzung verwenden (anders als ein Host-PC).

ISP-Einstellungen

Geben Sie den von Ihrem ISP mitgeteilten Benutzernamen, das Passwort und sonstige Authentisierungsparameter ein. Falls Sie ständig mit dem Internet verbunden sein möchten, wählen Sie **Immer in Betrieb**.

Benutzername – Geben Sie den vom ISP mitgeteilten Benutzernamen in diesem Feld ein.

Passwort – Geben Sie das vom ISP mitgeteilte Passwort in diesem Feld ein.

PPP-Authentifizierung – Wählen Sie für PPP entweder **Nur PAP** oder **PAP oder CHAP**.

Max. Leerlaufzeit – Stellen Sie die Leerlaufzeit ein, nach der die Internet-Verbindung abgebrochen werden soll. Diese Einstellung ist nur aktiv, wenn die Betriebsart **Aktiv nach Bedarf** unter **WAN>> Basiskonfiguration** gewählt ist.

IP-Adresse vom ISP

Normalerweise weist der ISP Ihnen dynamisch IP-Adressen zu, wenn Sie sich verbinden und eine Anforderung senden. Einige ISPs bieten einen Service, wobei Sie bei jeder Anforderung die gleiche IP-Adresse zugewiesen bekommen können. In diesem Fall können Sie diese IP-Adresse im Feld Feste IP eintragen. Bitte wenden Sie sich an Ihren ISP, bevor Sie diese Funktion verwenden.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen **Aktiv**. Dann klicken Sie auf **OK**, um den Dialog zu verlassen.



Feste IP – Klicken Sie auf **Ja**, um diese Funktion zu nutzen, und geben Sie im Feld **Feste IP-Adresse** eine feste IP-Adresse ein.

Standard-MAC-Adresse – Sie können entweder die **Standard-MAC-Adresse** verwenden oder im entsprechenden Feld eine andere MAC-Adresse für den Router angeben.

MAC-Adresse selbst definieren – Geben Sie die MAC-Adresse für den Router manuell ein.

Index (1-15) in Timerkonfiguration - Sie können für Ihre Anforderungen vier Timer einrichten. Alle Timer können im Voraus auf der Web-Seite **Anwendungen – Timer** eingestellt werden, und Sie können die Nummer verwenden, die Sie auf jener Web-Seite gesetzt haben.

Nach Abschluss aller Einstellungen klicken Sie auf **OK**, um diese zu aktivieren.

MPoA

MPoA ist eine Spezifikation, welche die Integration von ATM-Diensten in bestehenden LANs ermöglicht, die als Protokoll entweder Ethernet, Token Ring, oder TCP/IP verwenden. Das Ziel von MPoA ist, verschiedene LANs zu befähigen, einander über ein ATM-Backbone Pakete zu senden.

Um **MPoA** als das Zugriffsprotokoll des Internets zu verwenden, wählen Sie den **MPoA**-Modus. Die folgende Web-Seite erscheint:

Einwahl ins Internet >> MPoA (RFC1483/2684)

MPoA (RFC1483/2684) Einstellungen

MPoA ○ aktiv ⦿ inaktiv

DSL-Modem Einstellungen
Multi-PVC Kanal: Kanal 1
Kapselung: 1483 Bridged IP LLC
VPI: 0
VCI: 33
Modulation: Multimode

RIP-Protokoll
☐ aktiv

Bridge-Modus
☐ aktiv

WAN-IP Netzwerk-Einstellungen
○ Automatisches Beziehen einer IP-Adresse
Router-Name *
Domain-Name *
*: wird von einigen Anbietern benötigt
⦿ IP-Adresse definieren WAN-IP Alias
IP-Adresse: 0.0.0.0
Subnetz-Maske: 0.0.0.0
Gateway IP-Adresse: 0.0.0.0

⦿ Voreingestellte MAC-Adresse verwenden
○ MAC-Adresse selbst definieren
MAC-Adresse: 00 : 50 : 7F : 8F : FA : B9

DNS-Server-IP
Primäre IP-Adresse
Sekundäre IP-Adresse

OK

MPoA (RFC1483/2684)
Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren. Klicken Sie auf **Inaktiv**, so wird diese Funktion geschlossen, und alle auf dieser Seite vorgenommenen Einstellungen werden verworfen.

DSL-Modemeinstellungen
Konfigurieren Sie die für Ihren ISP erforderlichen DSL-Parameter. Diese sind unerlässlich, um zu Ihrem ISP eine DSL-Verbindung aufzubauen.

Multi-PVC-Kanal - Die hier angezeigte Auswahl wird von der Seite **Einwahl ins Internet** – **Multi PVC** bestimmt. **M-PVC-Kanal auswählen** bedeutet, dass keine Auswahl markiert wird.

Kapselung - Dropdown-Liste zur Auswahl des vom ISP bestimmten Typs.

VPI - Geben Sie den vom ISP mitgeteilten Wert ein.

VCI - Geben Sie den vom ISP mitgeteilten Wert ein.

RIP-Protokoll
RIP ist die Abkürzung für *Routing Information Protocol* (RFC1058), welches bestimmt, wie Router Routing-Tabelleninformationen austauschen. Klicken Sie auf **Aktiv**, um diese Funktion zu aktivieren.

Bridge-Modus
Falls Sie **Bridged IP** als Protokoll wählen, können Sie dieses Kästchen markieren, um die Funktion aufzurufen. Der Router wird als Bridge-Modem laufen.

WAN-IP-Netzwerkeinstellungen
Dieses Menü ermöglicht Ihnen, eine IP-Adresse automatisch zu beziehen oder manuell einzugeben.

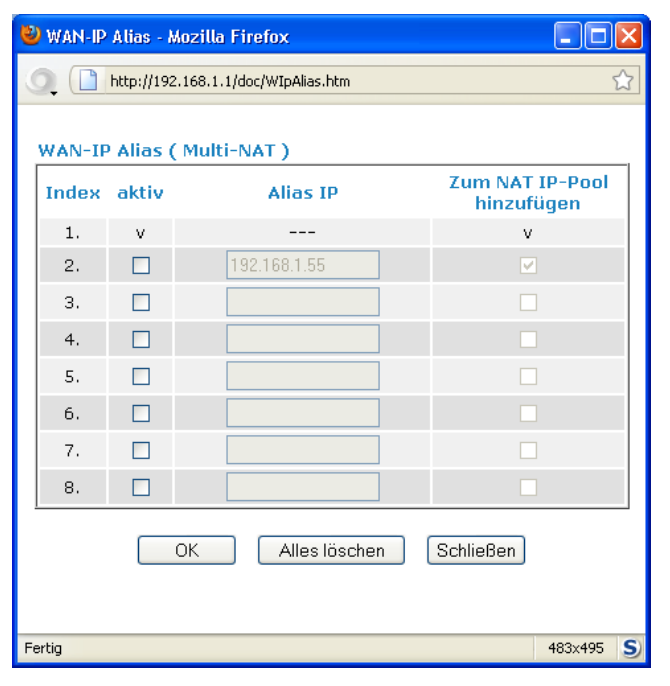
Automatisches Beziehen einer IP-Adresse – Klicken Sie auf diese Taste, um die IP-Adresse automatisch zu beziehen.

Router-Name – Geben Sie den vom ISP mitgeteilten Router-Namen ein.

Domain-Name – Geben Sie den zugewiesenen Domain-Namen ein.

IP-Adresse definieren – Klicken Sie auf diese Taste, um einige Daten einzugeben.

WAN-IP Alias - Falls Sie mehrere öffentliche IP-Adressen haben und diese an der WAN-Schnittstelle verwenden möchten, benutzen Sie bitte WAN-IP Alias. Sie können außer der aktuell verwendeten IP-Adresse bis zu acht öffentliche IP-Adressen einrichten. Bitte beachten Sie, dass diese Option lediglich für WAN1 verfügbar ist. Geben Sie die zusätzliche WAN IP-Adresse ein und markieren Sie das Kästchen **Aktiv**. Dann klicken Sie auf **OK**, um den Dialog zu verlassen.



IP-Adresse – Geben Sie die private IP-Adresse ein.

Subnetz-Maske – Geben Sie die Subnetz-Maske ein.

Gateway-IP-Adresse – Geben Sie die IP-Adresse des Gateways ein.

Standard-MAC-Adresse Geben Sie die MAC-Adresse für den Router ein. Sie können entweder die **Standard-MAC-Adresse** verwenden oder bei Bedarf eine andere MAC-Adresse angeben.

MAC-Adresse – Geben Sie die MAC-Adresse für den Router manuell ein.

DNS-Server-IP Geben Sie die bevorzugte IP-Adresse für den Router ein. Falls erforderlich, geben Sie eine alternative IP-Adresse ein.

Nach Abschluss aller Einstellungen klicken Sie auf **OK**, um diese zu aktivieren.

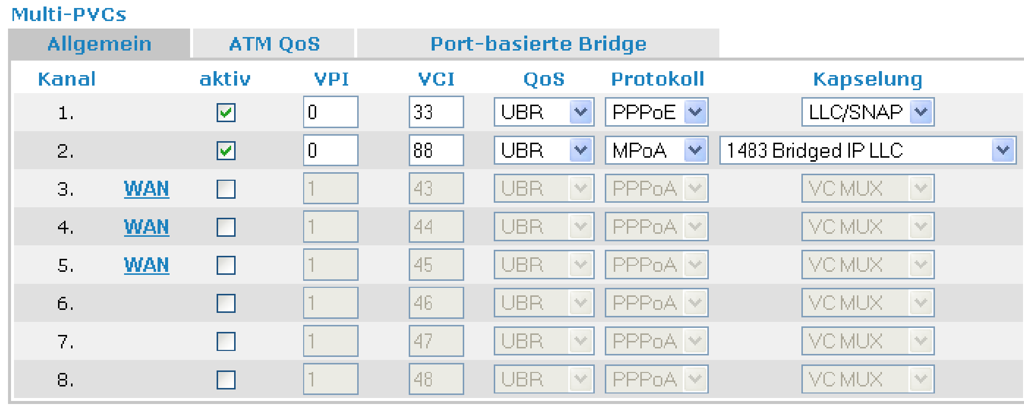
4.1.3 Multi-PVCs

Dieser Router ermöglicht Ihnen die Einrichtung von Multi-PVCs für verschiedene Datenübertragungen. Zur Konfiguration gehen Sie zu **Einwahl ins Internet** und wählen die Seite **Multi-PVC**.

Allgemein

Das System ermöglicht Ihnen, bis zu acht Kanäle, die als erste PVC-Leitung gewählt werden können, als Multi-PVCs zu bestimmen.

Einwahl ins Internet >> Multi-PVCs



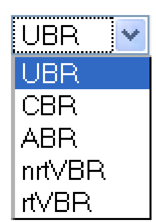


Aktiv Markieren Sie dieses Kästchen, um den Kanal zu aktivieren. Die hier aktivierten Kanäle werden in der Dropdown-Liste **Multi-PVC-Kanäle** auf der Web-Seite **Einwahl ins Internet** angezeigt. Obwohl Sie auf dieser Seite acht Kanäle aktivieren können, kann nur ein Kanal auf der Web-Seite **Einwahl ins Internet** gewählt werden.

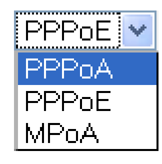
VPI Geben Sie den vom ISP mitgeteilten Wert ein.

VCI Geben Sie den vom ISP mitgeteilten Wert ein.

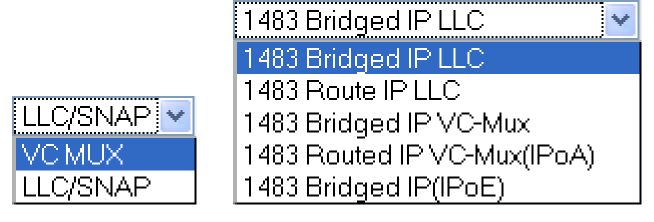
QoS-Typ Wählen Sie für den Kanal einen geeigneten QoS-Typ.



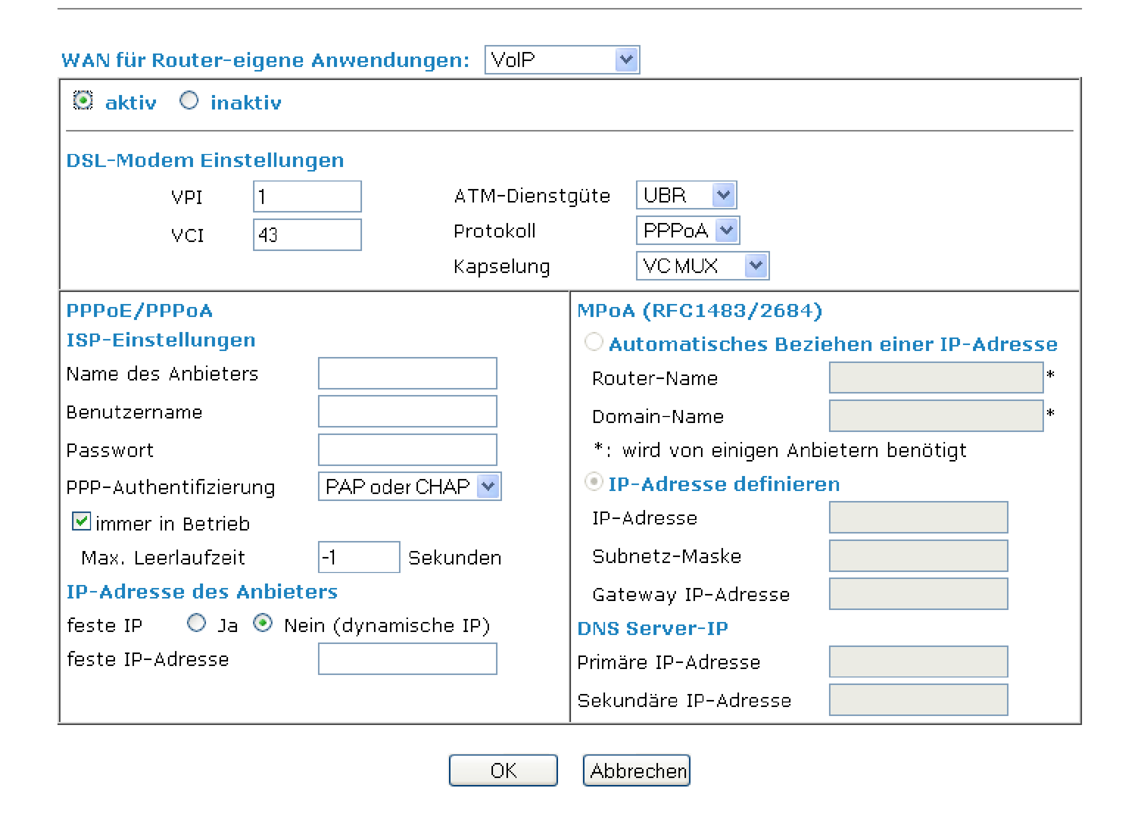
Protokoll Wählen Sie ein geeignetes Protokoll für diesen Kanal.



Kapselung Wählen Sie einen geeigneten Typ für diesen Kanal. Die Typen ändern sich je nach gewählter Protokolleinstellung.



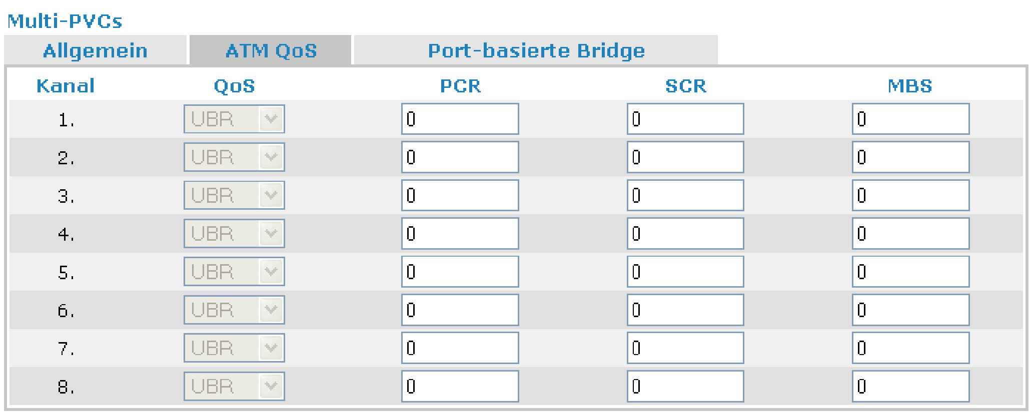
WAN-Verbindungen für die Kanäle 3, 4, 5 werden für Router-eigene Anwendungen wie TR-069 und VoIP bereitgestellt. Die notwendigen Einstellungen erhalten Sie von Ihrem ISP. Bei Bedarf wenden Sie sich bitte an Ihren ISP und klicken dann auf die WAN-Verbindung von Kanal 3, 4 oder 5, um Ihren Router zu konfigurieren.



ATM QoS

Diese Konfiguration bezieht sich auf die Upstream-Pakete. Die Information wird von Ihrem ISP bereitgestellt. Bitte wenden Sie sich für Einzelheiten an Ihren ISP.

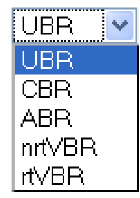
Einwahl ins Internet >> Multi-PVCs



Hinweis: 1. Der Eintrag "0" bedeutet Standardwert.
2.PCR(max) = ADSL Up Speed / 53 / 8.



QoS-Typ Wählen Sie für den Kanal einen geeigneten QoS-Typ gemäß der Information von Ihrem ISP.



PCR Abkürzung für Peak Cell Rate. Die Standardeinstellung ist "0".

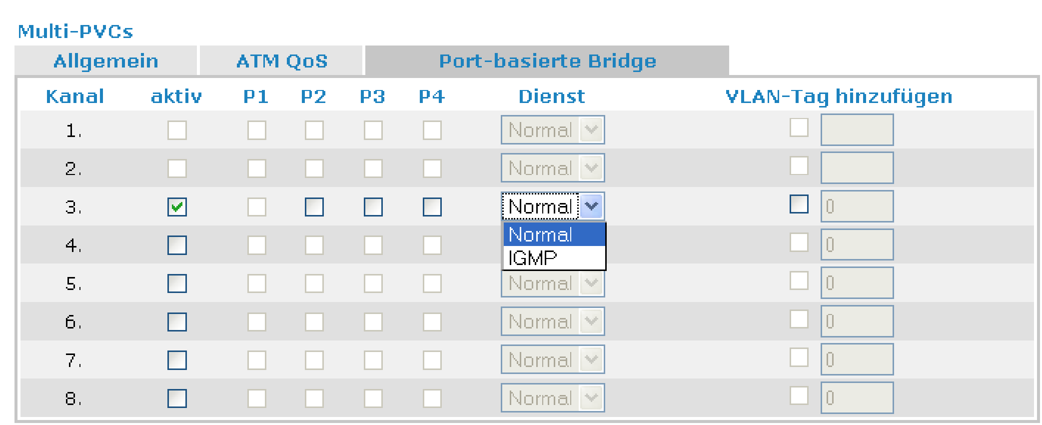
SCR Abkürzung für Sustainable Cell Rate. Der SCR-Wert muss kleiner als der PCR-Wert sein.

MBS Abkürzung für Maximum Burst Size. Der Wertebereich reicht von 10 bis 50.

Port-basierte Brücke

Auf der Seite **Allgemein** können Sie den ersten PVC einstellen. Zur Einstellung des zweiten PVC klicken Sie bitte auf den Reiter **Port-basierte Brücke**, um die Konfigurationsseite für die Brücke zu öffnen.

Einwahl ins Internet >> Multi-PVCs



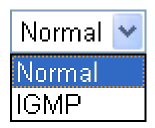
Hinweis: 1. Die Kanäle 1 und 2 sind reserviert für NAT/Routing.
2. P1 ist ebenfalls für NAT/Routing reserviert.



Aktiv — Markieren Sie dieses Kästchen, um den Kanal zu aktivieren. Auf dieser Seite können nur die Kanäle 3 bis 8 gesetzt werden, da die Kanäle 1 und 2 für NAT reserviert sind.

P1 bis P4 — Bezieht sich auf die LAN-Ports 1 bis 4. Markieren Sie das Kästchen, um die LAN-Ports für die Kanäle 3 bis 8 festzulegen.

Servicetyp — Normalerweise wird der Servicetyp für den Dienst des Video-Streams verwendet (z.B. IPTV). Er kann die Pakete der Fernsteuerung und des Video-Streams verschiedenen PVCs zuteilen. Meistens wird für die Fernsteuerung das IGMP-Protokoll benutzt.



Normal – Bedeutet, dass PVC alle Pakete außer IGMP annehmen kann.

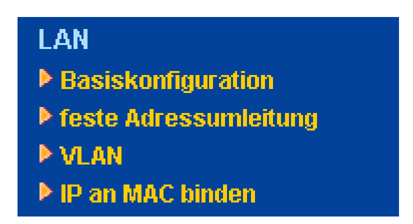
IGMP – Bedeutet, dass PVC lediglich IGMP-Pakete annehmen kann.

Tag hinzufügen — Um die Verwendung von PVC zu kennzeichnen, markieren Sie dieses Kästchen, um diese Einstellung zu aktivieren. Geben Sie die VLAN ID-Nummer ein.

Klicken Sie auf **Löschen**, um alle Konfigurationen auf dieser Seite zu entfernen, falls Sie mit diesen nicht zufrieden sind. Um die Konfiguration fertig zu stellen, klicken Sie auf **OK**, um die Einstellungen zu sichern und die Seite zu verlassen. Um die Konfiguration abzubrechen und die Seite zu verlassen, klicken Sie auf **Abbrechen**.

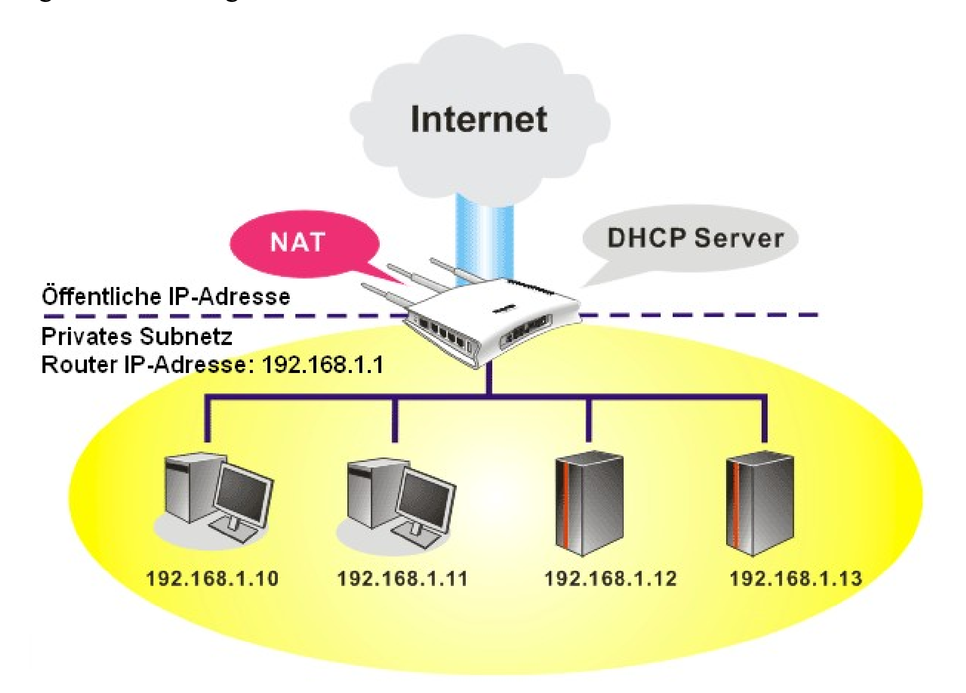
4.2 LAN

Das Local Area Network (LAN) ist eine Gruppe von Subnetzen, die vom Router verwaltet und gesteuert werden. Die Netzwerkstruktur hängt davon ab, welche Art von öffentlichen IP-Adressen Ihnen Ihr ISP zuweist.

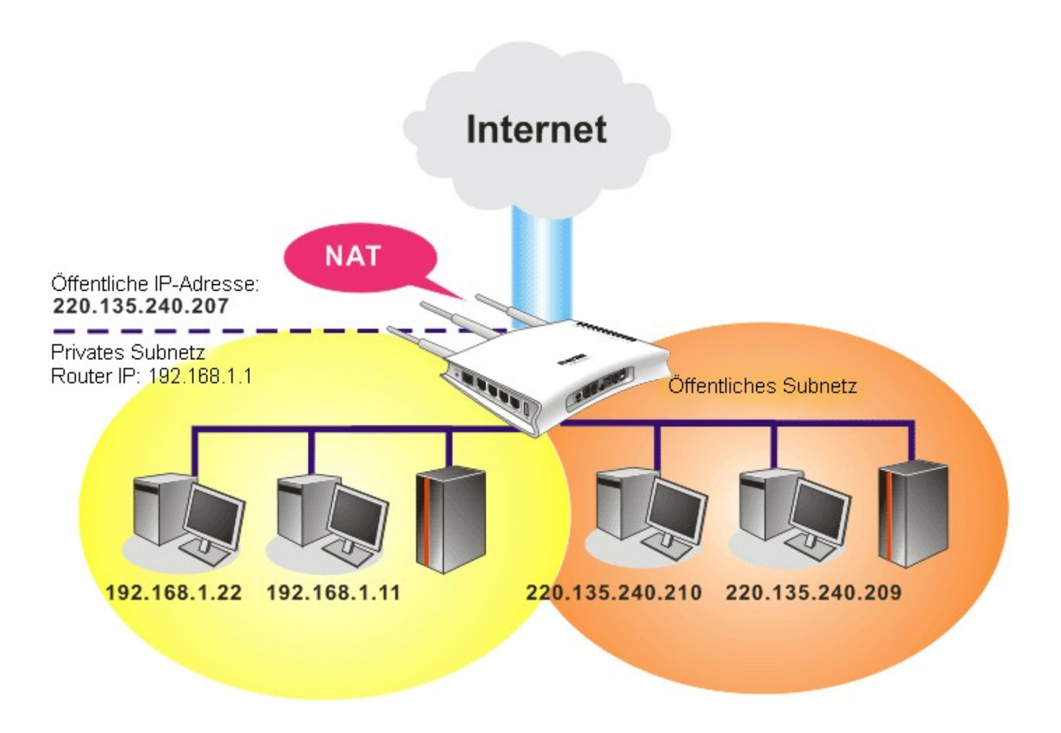


4.2.1 LAN-Grundlagen

Die grundlegende Funktion des Vigor-Routers ist NAT. Hiermit wird ein privates Subnetz aufgebaut. Wie bereits erwähnt, kommuniziert der Router über die öffentliche IP-Adresse mit anderen öffentlichen Hosts im Internet und über die private IP-Adresse mit lokalen Hosts. NAT hat die Aufgabe, die Pakete von der öffentlichen IP-Adresse auf private IP-Adressen umzuschreiben und die entsprechenden Pakete zum richtigen Host und umgekehrt weiterzuleiten. Außerdem verfügt der Vigor-Router über einen eingebauten DHCP-Server, der jedem lokalen Host private IP-Adressen zuweist. Die folgende Abbildung dient dem besseren Verständnis:



In einigen Sonderfällen können Sie von Ihrem ISP ein öffentliches IP-Subnetz wie 220.135.240.0/24 erhalten. Dies bedeutet, dass Sie ein öffentliches Subnetz einrichten können oder ein zweites Subnetz bestimmen können, in dem jeder Host eine öffentliche IP-Adresse erhält. Als Teil des öffentlichen Subnetzes ist der Vigor-Router für das IP-Routing verantwortlich, um Hosts im öffentlichen Subnetz zu ermöglichen, mit anderen öffentlichen Hosts oder Servern zu kommunizieren, die außerhalb liegen. Deswegen sollte der Router als Gateway für öffentliche Hosts eingerichtet werden.



Was ist das Routing Information Protocol (RIP)?

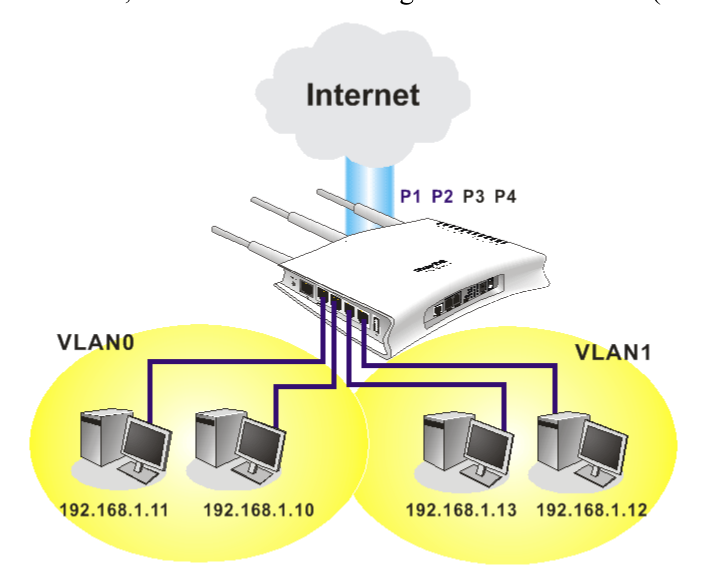
Der Vigor-Router tauscht mit Hilfe von RIP Routing-Informationen mit benachbarten Routern aus, um IP-Routing zu ermöglichen. Auf diese Weise benachrichtigen sich die Router automatisch, wenn Benutzer Daten des Routers ändern, z.B. die IP-Adresse.

Was ist eine feste Adressumleitung?

Falls Sie in Ihrem LAN mehrere Subnetze haben, sind **feste Adressumleitungen** die schnellste und effektivste Möglichkeit, Verbindungen herzustellen. Sie können einfach Regeln für die Weiterleitung von Daten aus einem angegebenen Subnetz in ein anderes angegebenes Subnetz festlegen, ohne RIP zu verwenden.

Was sind virtuelle LANs?

Sie können lokale Hosts nach physischen Ports gruppieren und bis zu vier virtuelle LANs einrichten. Um die Kommunikation zwischen verschiedenen Gruppen zu verwalten, setzen Sie bitte die Regeln im Virtual LAN (VLAN) Menü.



4.2.2 Basiskonfiguration

Diese Seite beinhaltet die allgemeinen LAN-Einstellungen.

Klicken Sie auf **LAN**, um die Seite mit den LAN-Einstellungen zu öffnen, und wählen Sie **Basiskonfiguration**.

LAN >> Basiskonfiguration

Ethernet TCP / IP und DHCP

LAN-Konfiguration
NAT:
NAT IP-Adresse 192.168.1.1
NAT Subnetz-Maske 255.255.255.0
IP-Routing ○ aktiv ⦿ inaktiv
Routing IP-Adresse 192.168.2.1
Subnetz-Maske 255.255.255.0
Routing DHCP-Server
RIP inaktiv

DHCP-Server
⦿ aktiv ○ inaktiv
Relay-Agent-Subnetz: ○ NAT-Subnetz ○ Routing-Subnetz
Start-IP-Adresse 192.168.1.10
IP-Pool (max. Anzahl) 50
Gateway IP-Adresse 192.168.1.1
DHCP-Server-IP für Relay-Agent

DNS-Server-IP
☐ Folgende DNS-Einstellungen verwenden
Primäre IP-Adresse
Sekundäre IP-Adresse

OK

NAT IP-Adresse Geben Sie die private IP-Adresse für die Verbindung zu einem lokalen privaten Netzwerk ein (Standard: 192.168.1.1).

Subnetz-Maske Geben Sie den Adressbereich ein, der die Größe des Netzwerks bestimmt (Standard: 255.255.255.0/ 24).

IP-Routing Klicken Sie auf **Aktiv**, um diese Funktion zu starten. Die Standardeinstellung ist **Inaktiv**.

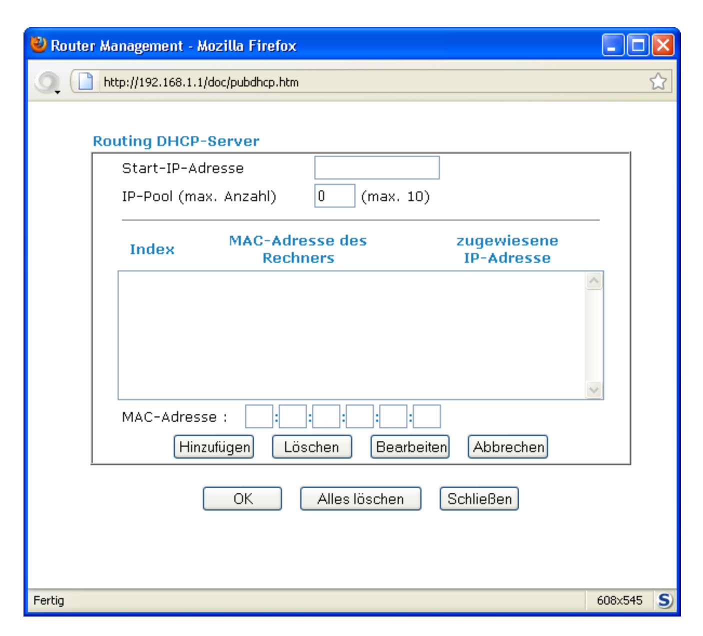
Routing IP-Adresse Geben Sie die 2. IP-Adresse für die Verbindung zu einem Subnetz ein.

(Standard: 192.168.2.1/ 24)

Subnetz-Maske Ein Adressbereich, der die Größe des Netzwerks bestimmt.

(Standard: 255.255.255.0/ 24)

Routing DHCP-Server Sie können den Router als DHCP-Server für das zweite Subnetz einrichten.



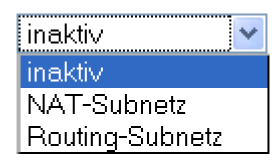
Start-IP-Adresse: Geben Sie einen Wert aus dem IP-Adresspool an, bei dem der DHCP-Server bei der Vergabe von IP-Adressen anfangen soll. Falls die Routing-IP-Adresse Ihres Routers 220.135.240.1 ist, muss die Start-IP-Adresse 220.135.240.2 oder größer, jedoch kleiner als 220.135.240.254 sein.

IP-Pool (Anzahl): Geben Sie die Anzahl der IP-Adressen in diesem Pool an. Die maximale Anzahl beträgt 10. Wenn Sie zum Beispiel 3 eingeben und die Routing-IP-Adresse Ihres Routers 220.135.240.1 ist, so reicht der IP-Adressbereich des DHCP-Servers von 220.135.240.2 bis 220.135.240.4.

MAC-Adresse: Geben Sie die MAC-Adressen der Hosts nacheinander ein und klicken Sie auf **Hinzufügen**, um eine Liste der Hosts zu erstellen, denen aus dem oben erwähnten Pool IP-Adressen zugewiesen, gelöscht oder geändert werden sollen. Die Erstellung einer Liste von MAC-Adressen für den Routing-DHCP-Server ermöglicht dem Router, den richtigen Hosts die richtigen IP-Adressen des richtigen Subnetzes zuzuweisen. So wird vermieden, dass den Hosts im Routing-Subnetz IP-Adressen aus dem NAT-Subnetz zugewiesen werden.

RIP

Inaktiv deaktiviert das RIP-Protokoll. Damit wird zwischen Routern keine Routing-Information ausgetauscht. (Standardeinstellung)



NAT-Subnetz - Lässt den Router die RIP-Information des NAT-Subnetzes mit benachbarten Routern austauschen.

Routing-Subnetz - Lässt den Router die RIP-Information des Routing-Subnetzes mit benachbarten Routern austauschen.

DHCP-Serverkonfiguration

DHCP ist die Abkürzung für Dynamic Host Configuration Protocol. Der Router dient standardmäßig als DHCP-Server für Ihr Netzwerk und sendet automatisch IP-bezogene Einstellungen an alle lokalen Rechner, die als DHCP-Clients konfiguriert sind. Es wird empfohlen, den Router als DHCP-Server aktiviert zu

lassen, sofern Sie für Ihr Netzwerk keinen gesonderten DHCP-Server haben.

Falls Sie im Netzwerk nicht den Vigor-Router, sondern einen anderen Rechner als DHCP-Server benutzen möchten, können Sie den Relay-Agent verwenden, um die DHCP-Anforderungen an den jeweiligen Rechner umzuleiten.

Aktiv - Lässt den Router jedem Host im LAN IP-Adressen zuweisen.

Inaktiv – Lässt Sie manuell jedem Host im LAN IP-Adressen zuweisen.

Relay-Agent – (NAT-Subnetz/Routing-Subnetz) Geben Sie das Subnetz an, in dem sich der DHCP-Server befindet, an den der Relay-Agent die DHCP-Anforderungen weiterleiten soll.

Start-IP-Adresse - Geben Sie einen Wert aus dem IP-Adresspool an, bei dem der DHCP-Server bei der Vergabe von IP-Adressen anfangen soll. Falls die erste IP-Adresse Ihres Routers 192.168.1.1 ist, muss die Start-IP-Adresse 192.168.1.2 oder größer, jedoch kleiner als 192.168.1.254 sein.

IP-Pool (Anzahl) - Geben Sie die maximale Anzahl der Rechner an, denen der DHCP-Server IP-Adressen zuweisen soll. Der Standardwert beträgt 50, und die maximale Anzahl ist 253.

Gateway-IP-Adresse - Geben Sie die Gateway-IP-Adresse für den DHCP-Server ein. Der Wert entspricht üblicherweise der ersten IP-Adresse des Routers, d.h. der Router ist das Standard-Gateway.

DHCP-Server-IP für Relay-Agent - Setzen Sie die IP-Adresse des DHCP-Servers, den Sie verwenden möchten, damit der Relay-Agent die DHCP-Anforderungen an diesen DHCP-Server weiterleiten kann.

DNS-Serverkonfiguration

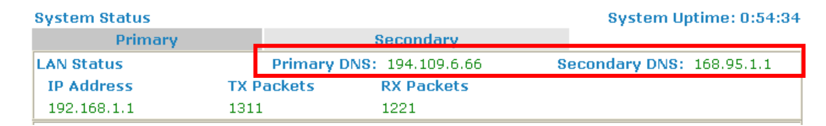
DNS ist die Abkürzung für Domain Name System. Jeder Internet-Host muss eine eindeutige IP-Adresse haben und kann auch einen Namen tragen, der einfach zu merken ist, wie z.B. www.yahoo.com. Der DNS-Server wandelt den benutzerfreundlichen Namen in die entsprechende IP-Adresse um.

Folgende DNS-Einstellungen verwenden - Den Vigor-Router zwingen, nicht die vom Internetzugangsserver bestimmten DNS-Server (PPPoE, PPTP, L2TP oder DHCP-Server), sondern die DNS-Server auf dieser Seite zu verwenden.

Primäre IP-Adresse - Geben Sie hier die IP-Adresse eines DNS-Servers ein, dessen Daten Ihnen Ihr ISP mitgeteilt haben sollte. Falls der ISP diese Daten nicht bereitstellt, trägt der Router automatisch die IP-Adresse des Standard-DNS-Servers in diesem Feld ein: 194.109.6.66.

Sekundäre IP-Adresse - Hier können Sie eine alternative DNS-Server-IP eintragen, falls der ISP Ihnen die Daten mehrerer DNS-Server mitgeteilt hat. Falls der ISP diese Daten nicht bereitstellt, trägt der Router automatisch die IP-Adresse des standardmäßigen alternativen DNS-Servers in diesem Feld ein: 194.98.0.1.

Die Standard-DNS-Server-IP ist unter dem Onlinestatus sichtbar:



Falls die Felder für die IP-Adressen des bevorzugten DNS-Servers und des alternativen DNS-Servers nicht ausgefüllt werden, weist der Router seine eigene IP-Adresse als DNS-Proxy-Server für lokale Benutzer zu und unterhält einen DNS-Cache.

Falls die IP-Adresse eines Domain-Namens bereits im DNS-Cache vorhanden ist, löst der Router den Domain-Namen sofort auf. Andernfalls leitet der Router die DNS-Anfrage über die WAN-Verbindung (z.B. DSL, Kabel) an den externen DNS-Server weiter.

In Kapitel 4 werden zwei übliche Szenarien für LAN-Einstellungen vorgestellt. Neben Einzelheiten zu den Konfigurationsbeispielen enthält das Kapitel weitere Informationen für Ihre Bedürfnisse.

4.2.3 Feste Adressumleitung

Gehen Sie zur Seite mit den Einstellungen für das **LAN** und wählen Sie **Feste Adressumleitung**.

LAN >> feste Adressumleitung

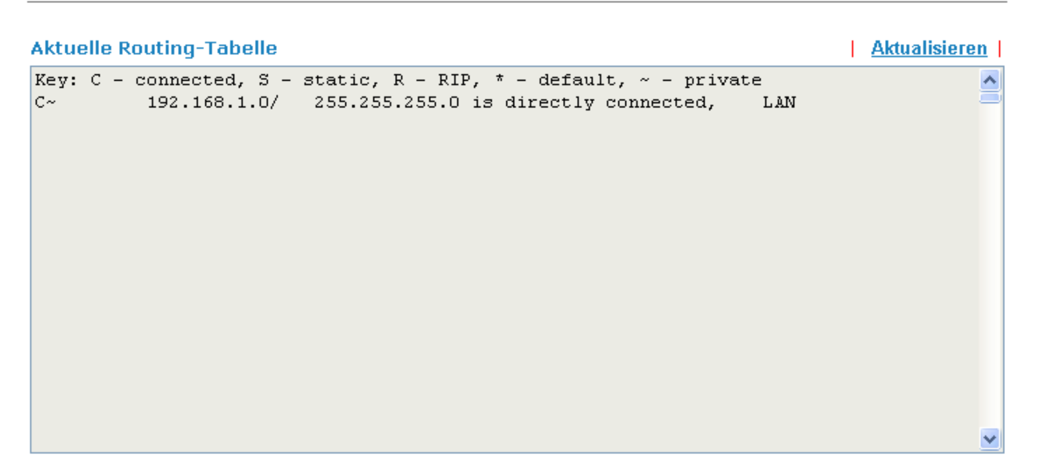
Konfiguration der festen Route | Auf Werkseinstellungen zurücksetzen | Routing-Tabelle |

Index	Ziel-Adresse	Status	Index	Ziel-Adresse	Status
1.	???	?	6.	???	?
2.	???	?	7.	???	?
3.	???	?	8.	???	?
4.	???	?	9.	???	?
5.	???	?	10.	???	?

Status: v --- aktiv, x --- inaktiv, ? --- leer

Index	Die Nummern 1 bis 10 unter Index ermöglichen Ihnen, auf die nächste Seite zu gelangen, um die feste Adressumleitung einzurichten.
Zieladresse	Zeigt die Zieladresse der festen Adressumleitung an.
Status	Zeigt den Status der festen Adressumleitung an.
Auf Werkseinstellungen zurücksetzen	Alle Profile löschen.
Routing-Tabelle anzeigen	Zeigt die Routing-Tabelle an.

Diagnose-Tools >> Routing-Tabelle

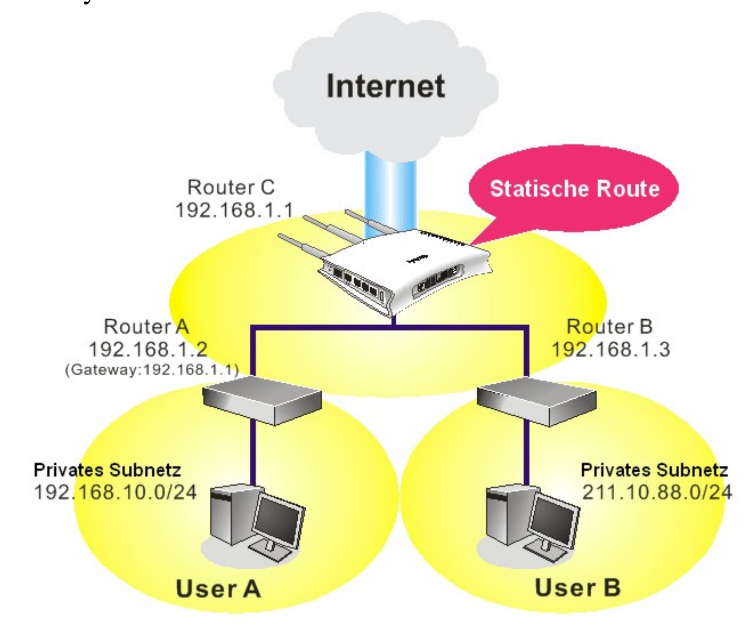


Hinzufügen von festen Adressumleitungen zu privaten und öffentlichen Netzwerken

Es folgt ein Konfigurationsbeispiel für eine feste Adressumleitung im Hauptrouter, so dass die Benutzer A und B, die sich in unterschiedlichen Subnetzen befinden, über den Router miteinander kommunizieren können. Es wird angenommen, dass der Internetzugang bereits eingerichtet worden ist und der Router ordnungsgemäß funktioniert.

- Der Hauptrouter wird zum Surfen im Internet verwendet.
- Einrichtung eines privaten Subnetzes 192.168.10.0 mit dem internen Router A (192.168.1.2)
- Einrichtung eines öffentlichen Subnetzes 211.100.88.0 über den internen Router B (192.168.1.3).
- Konfiguration des Hauptrouters 192.168.1.1 als Standard-Gateway für den Router A (192.168.1.2).

Vor Einrichtung der festen Adressumleitung kann Benutzer A nicht mit Benutzer B kommunizieren, da Router A nur anerkannte Pakete an den Hauptrouter als Standard-Gateway leiten kann.



1. Gehen Sie zur **LAN**-Seite, klicken auf **Basiskonfiguration** und wählen das erste Subnetz als **RIP**. Klicken Sie dann auf **OK**.

> **Hinweis:** Es gibt zwei Gründe für die Anwendung von RIP im ersten Subnetz. Der erste ist, dass die LAN-Schnittstelle über das erste Subnetz (192.168.1.0/24) RIP-Pakete mit benachbarten Routern austauschen kann. Der zweite Grund besteht darin, dass diese Hosts in internen privaten Subnetzen (z.B. 192.168.10.0/24) über den Router auf das Internet zugreifen können und ständig IP-Routing-Informationen mit anderen Subnetzen austauschen können.

2. Wählen Sie **LAN - Feste Adressumleitung** und klicken Sie auf die **Indexnummer 1**. Markieren Sie das Kästchen **Aktiv**. Fügen Sie wie unten gezeigt eine feste Adressumleitung hinzu, die festlegt, dass alle für 192.168.10.0 bestimmten Pakete an 192.168.1.2 umgeleitet werden. Klicken Sie auf **OK**.

LAN >> feste Adressumleitung

Index-Nr. 1

☑ aktiv

IP-Zieladresse	192.168.10.0
Subnetz-Maske	255.255.255.0
Gateway IP-Adresse	192.168.1.2
Netzwerkschnittstelle	LAN

OK Abbrechen

3. Kehren Sie zurück zur Seite **Feste Adressumleitung**. Klicken Sie auf eine andere **Indexnummer**, um wie unten gezeigt eine weitere feste Adressumleitung hinzuzufügen, die festlegt, dass alle für 211.100.88.0 bestimmten Pakete an 192.168.1.3 umgeleitet werden.

LAN >> feste Adressumleitung

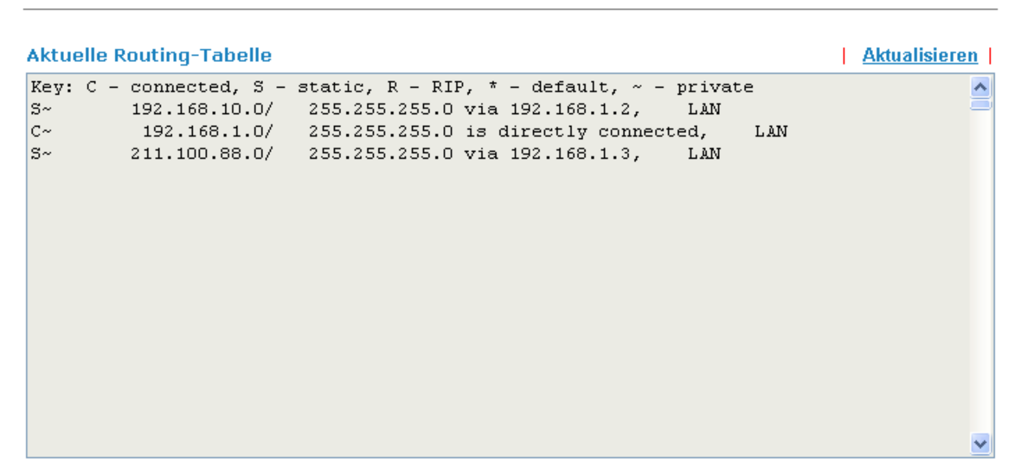
Index-Nr. 1

☑ aktiv

IP-Zieladresse	211.100.88.0
Subnetz-Maske	255.255.255.0
Gateway IP-Adresse	192.168.1.3
Netzwerkschnittstelle	LAN

OK Abbrechen

4. Gehen Sie zu **Diagnose-Tools** und wählen Sie **Routing-Tabelle**, um die aktuelle Routing-Tabelle zu verifizieren.

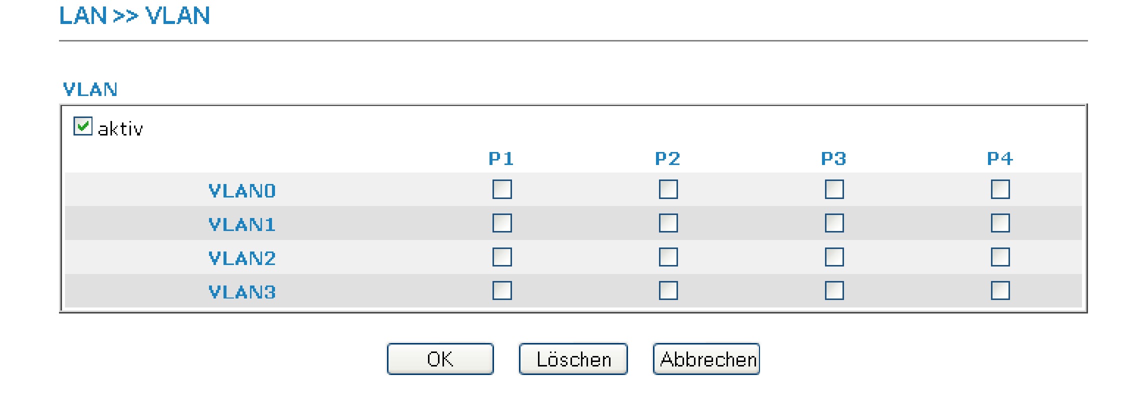

Diagnose-Tools >> Routing-Tabelle

Aktuelle Routing-Tabelle | Aktualisieren |

```
Key: C - connected, S - static, R - RIP, * - default, ~ - private
S~       192.168.10.0/   255.255.255.0 via 192.168.1.2,    LAN
C~        192.168.1.0/   255.255.255.0 is directly connected,    LAN
S~       211.100.88.0/   255.255.255.0 via 192.168.1.3,    LAN
```

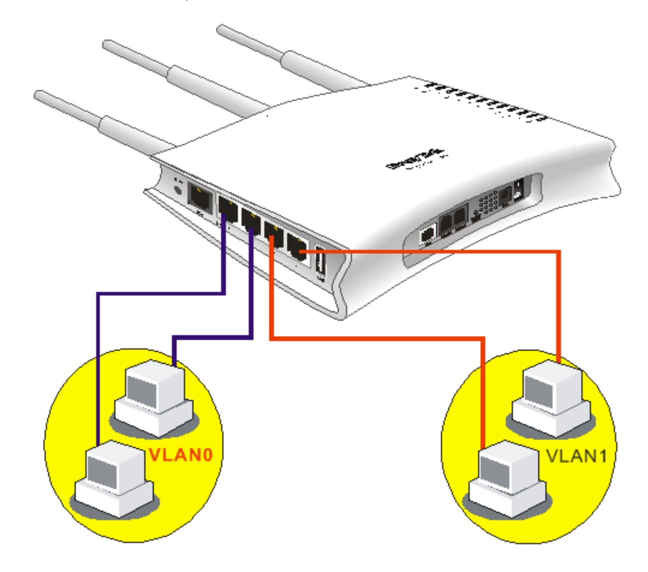
4.2.4 VLAN

Die Virtual LAN Funktion bietet eine komfortable Möglichkeit, Hosts zu verwalten, indem diese auf der Grundlage des physischen Ports gruppiert werden. Gehen Sie zur **LAN**-Seite und wählen Sie **VLAN**. Die folgende Seite erscheint. Klicken Sie auf **Aktiv**, um die VLAN-Funktion zu starten.

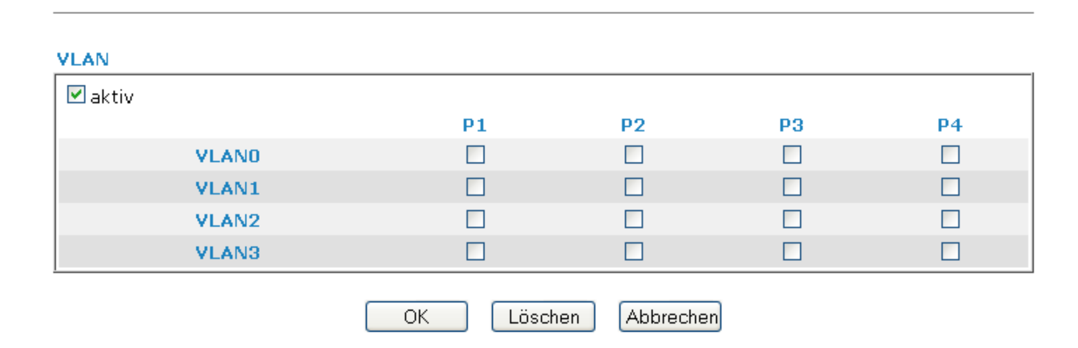


Das folgende Beispiel zeigt, wie man ein VLAN hinzufügen oder entfernen kann.

1. Falls VLAN 0 aus Hosts besteht, die mit P1 und P2 verbunden sind, so besteht VLAN 1 aus Hosts, die mit P3 und P4 verbunden sind.



2. Haken Sie das Kästchen zur Aktivierung der VLAN-Funktion an und markieren Sie die unten gezeigte Tabelle gemäß Ihren Anforderungen.



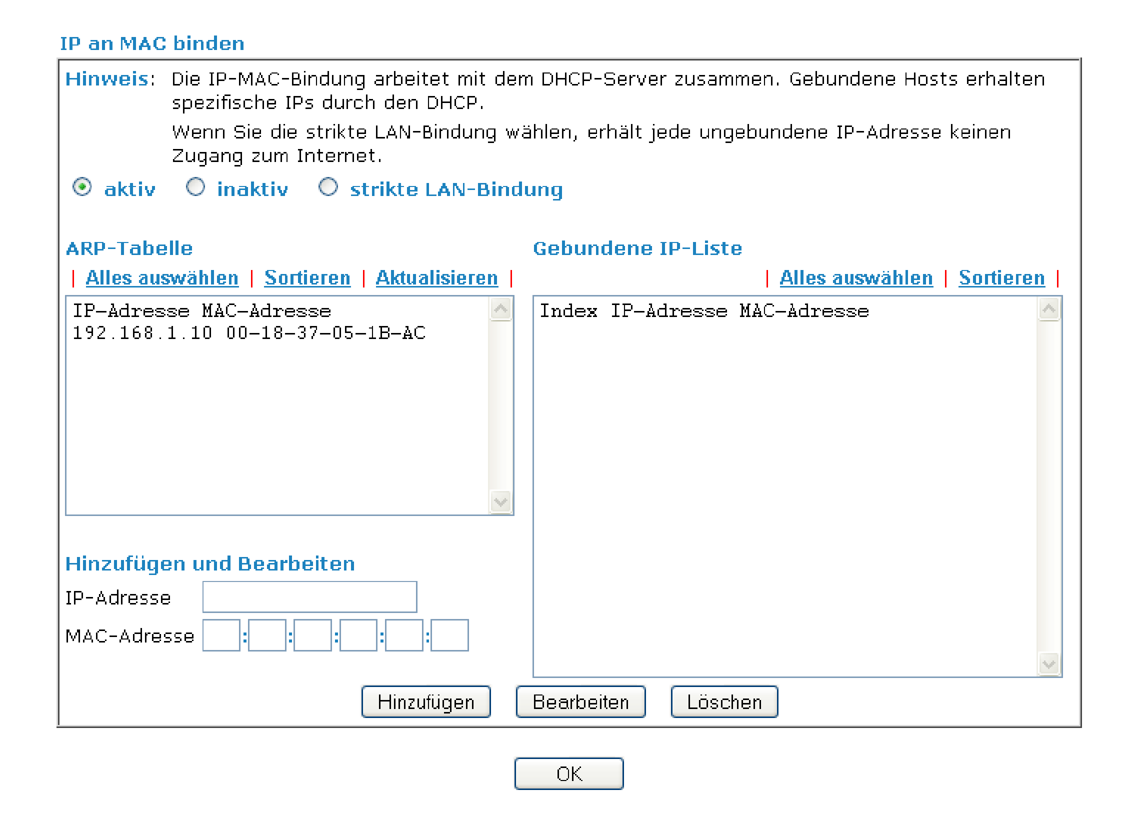
Um VLAN zu entfernen, deaktivieren Sie das entsprechende Kästchen und klicken auf **OK**, um das Ergebnis zu speichern.

4.2.5 IP an MAC binden

Diese Funktion wird verwendet, um zwecks besserer Kontrolle im LAN die IP-Adresse an die MAC-Adresse zu binden. Falls diese Funktion aktiviert ist, können die zugewiesenen IP-/MAC-Bindungen nicht geändert werden. Änderungen der gebundenen IP- bzw. MAC-Adresse können dazu führen, dass Ihr Zugriff auf das Internet blockiert wird.

Klicken Sie auf **LAN** und wählen Sie **IP an MAC binden**, um die Seite mit den Einstellungen zu öffnen.

LAN >> IP an MAC binden



Aktiv	Klicken Sie auf diese Taste, um diese Funktion zu aktivieren. Es können jedoch auch IP-/MAC-Paare, die nicht in der Liste aufgeführt sind, auf das Internet zugreifen.
Inaktiv	Klicken Sie auf diese Taste, um diese Funktion zu deaktivieren. Alle Einstellungen auf dieser Seite werden ungültig.
Strikte LAN-Bindung	Klicken Sie auf diese Taste, um IP-/MAC-Bindungen zu blockieren, die nicht in der Liste aufgeführt sind.
ARP-Tabelle	Dies ist die LAN ARP-Tabelle dieses Routers. Die IP- und MAC-Information erscheint in diesem Feld. Jedes in der ARP-Tabelle aufgeführte IP-/MAC-Paar kann ausgewählt und durch Klicken auf **Hinzufügen** der gebundenen IP-Liste hinzugefügt werden.
Hinzufügen und bearbeiten	**IP-Adresse** - Geben Sie die IP-Adresse ein, die für die angegebene MAC-Adresse zu verwenden ist.
	MAC-Adresse - Geben Sie die MAC-Adresse ein, die an die entsprechende IP-Adresse gebunden werden soll.

Aktualisieren	Klicken Sie hier, um die ARP-Tabelle zu aktualisieren. Wenn dem LAN ein neuer Rechner hinzugefügt wird, können Sie hier klicken, um die aktuellen Informationen in der ARP-Tabelle zu sehen.
Gebundene IP-Liste	Zeigt eine Liste der IP-Adressen an, die an MAC-Adressen gebunden sind.
Hinzufügen	Mit dieser Aktion können Sie das aus der ARP-Tabelle gewählte oder unter **Hinzufügen und bearbeiten** eingegebene IP/MAC-Paar der Tabelle **Gebundene IP-Liste** hinzufügen.
Bearbeiten	Ermöglicht Ihnen, die gewählte IP-Adresse und die MAC-Adresse zu bearbeiten und zu ändern, die Sie zuvor erstellt hatten.
Entfernen	Sie können jeden Eintrag aus der **Gebundenen IP-Liste** entfernen. Zur Auswahl klicken Sie einfach einen Eintrag an und klicken auf **Entfernen**. Der gewählte Eintrag wird aus der **Gebundenen IP-Liste** entfernt.

Hinweis: Bevor Sie **Strikte LAN-Bindung** wählen, müssen Sie einen IP-/MAC-Adresssatz für einen PC binden. Falls dies nicht geschieht, kann keiner der Rechner auf das Internet zugreifen. Außerdem mag es unmöglich sein, auf das Router-Menü zuzugreifen.

4.3 NAT

Normalerweise dient der Router als NAT-Router (Network Address Translation). Der NAT-Mechanismus ermöglicht die Verwendung von einer oder mehreren privaten IP-Adressen mit einer öffentlichen IP-Adresse. Die öffentliche IP-Adresse wird gewöhnlich von Ihrem ISP zugewiesen, was kostenpflichtig sein kann. Private IP-Adressen werden nur zwischen internen Hosts erkannt.

Wenn abgehende Pakete, die an einen öffentlichen Server im Internet gerichtet sind, beim NAT-Router ankommen, ändert der Router deren Quelladresse in die öffentliche IP-Adresse des Routers, wählt den verfügbaren Port und leitet die Pakete weiter. Gleichzeitig macht der Router in einer Tabelle einen Eintrag, um sich diese Adress-/Portzuordnung zu merken. Wenn der öffentliche Server antwortet, ist der eingehende Verkehr natürlich an die öffentliche IP-Adresse des Routers gerichtet, weshalb der Router anhand der Tabelle die Umwandlung vornimmt. So ist es einem internen Host möglich, flüssig mit einem externen Host zu kommunizieren.

Einige Vorteile von NAT:

- **Einsparung von Kosten für öffentliche IP-Adressen und effizienter Einsatz der IP-Adresse.** NAT ermöglicht die Übersetzung der internen IP-Adressen lokaler Hosts in eine einzige öffentliche IP-Adresse, so dass für sämtliche interne Hosts lediglich eine IP-Adresse erforderlich ist.
- **Höhere Sicherheit des internen Netzwerks durch Verdeckung der internen IP-Adresse.** Es gibt viele Arten von Angriffen auf Grundlage der IP-Adresse. Da der Angreifer die internen IP-Adressen nicht kennt, stellt die NAT-Funktion einen Schutz für das interne Netzwerk dar.

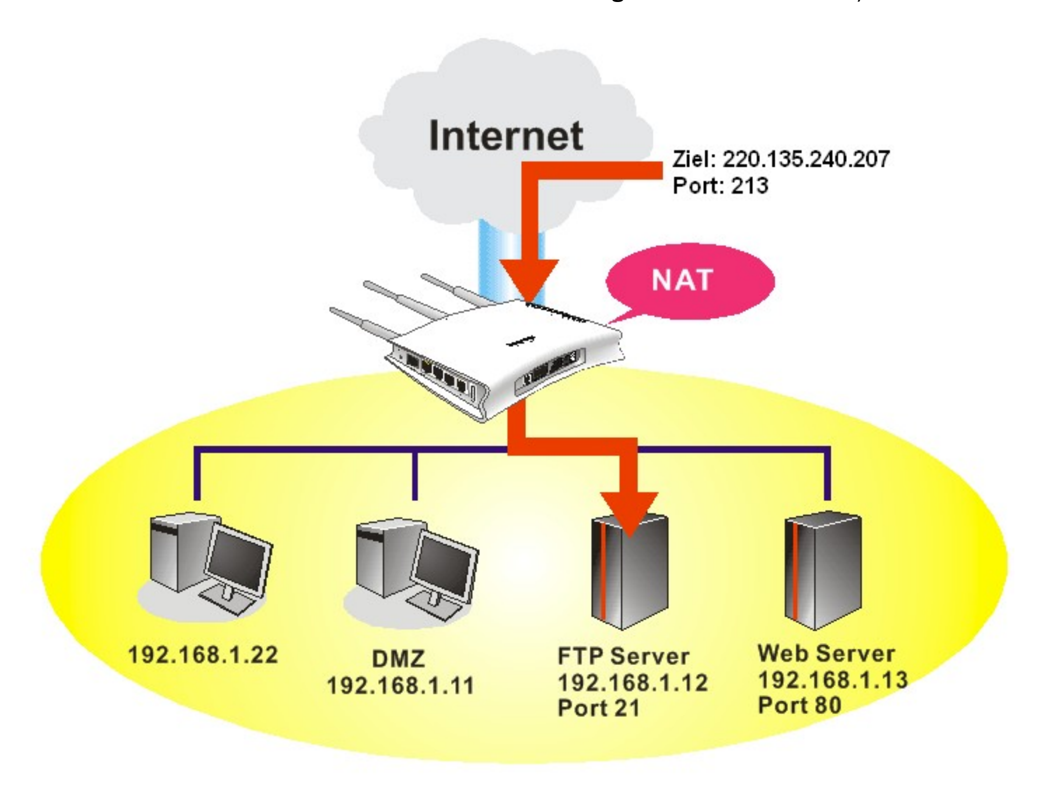
Auf der NAT-Seite sehen Sie die in RFC-1918 definierte private IP-Adresse. Normalerweise wird das Subnetz 192.168.1.0/24 für den Router verwendet. Wie oben erwähnt, kann die NAT-Funktion verschiedenen Diensten eine oder mehrere IP-Adressen oder Ports zuordnen, d.h. die NAT-Funktion verwendet Port-Zuordnungsmethoden.

Die folgende Abbildung zeigt die Menüeinträge für NAT:



4.3.1 Portumleitung

Portumleitung wird gewöhnlich für serverbezogene Dienste im lokalen Netzwerk genutzt, z.B. für Web-Server, FTP-Server, E-Mail-Server, usw. Meistens benötigen Sie für jeden Server eine öffentliche IP-Adresse, und diese öffentliche IP-Adresse/Domain-Name wird von allen Benutzern erkannt. Da der Server sich jedoch innerhalb des LANs befindet, das Netzwerk vom NAT des Routers geschützt wird und unter seiner privaten IP-Adresse/Port identifiziert wird, besteht der Zweck der Portumleitung darin, alle Zugriffe mit öffentlicher IP-Adresse von externen Benutzern an die private IP-Adresse/Port des Servers umzuleiten.



Die Portumleitung ist nur für eingehenden Datenverkehr möglich.

Um diese Funktion zu nutzen, gehen Sie zur **NAT**-Seite und wählen **Portumleitung**. Die **Portumleitungstabelle** ermöglicht 20 Port-Zuordnungseinträge für die internen Hosts.

NAT >> Portumleitung

Portumleitung | Auf Werkseinstellungen zurücksetzen |

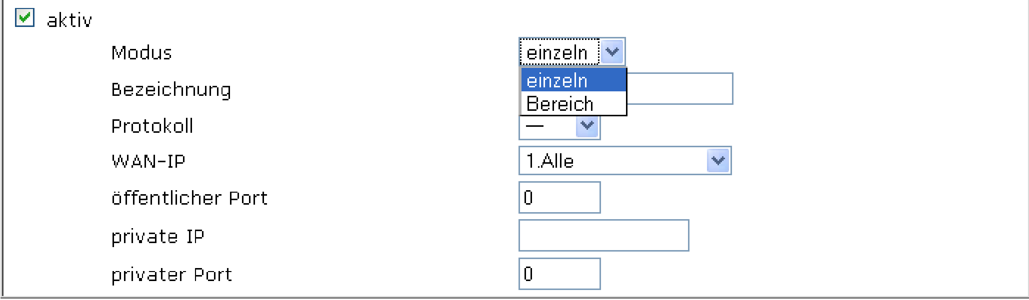
Index	Bezeichnung	öffentlicher Port	private IP	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 >> Weiter >>

Klicken Sie auf eine beliebige Nummer unter "Index" um auf die nächste Seite für die Konfiguration der Portumleitung zu gelangen.

NAT >> Portumleitung

Index-Nr. 1



Hinweis: Im Modus "Bereich" wird die End-IP automatisch berechnet, sofern Start-IP und der öffentliche Portbereich definiert wurden.

OK Löschen Abbrechen

Aktiv	Markieren Sie dieses Kästchen, um die Portumleitung zu aktivieren.
Modus	Es stehen hier zwei Optionen (**Einzeln** und **Bereich**) zur Auswahl. Um für den Dienst einen Bereich zu bestimmen, wählen Sie **Bereich**. Bei Eingabe der öffentlichen Ports (Startport und Endport) und der Start-IP des privaten IP-Adressbereichs im Bereichsmodus berechnet das System automatisch die End-IP des privaten IP-Adressbereichs und zeigt diese an.
Bezeichnung	Geben Sie eine Beschreibung des jeweiligen Netzwerkdienstes ein.
Protokoll	Wählen Sie das Protokoll für die Transportschicht (TCP oder UDP).
WAN-IP	Bestimmen Sie die WAN-IP für die Portumleitung. Es stehen acht IP-Aliasse zur Auswahl, die für die Portumleitung verwendet werden können. Die Standardeinstellung ist **Alle**, was bedeutet, dass sämtliche eingehende Daten von jedem Port zum angegebenen IP-Adress- und Portbereich weitergeleitet werden.
Öffentlicher Port	Geben Sie an, welcher Port an die angegebene **private IP und Port** des internen Hosts umgeleitet werden soll. Falls Sie **Bereich** als Portumleitungsmodus wählen, sehen Sie in diesem Feld zwei Kästchen. Geben Sie die gewünschte Nummer im ersten Kästchen ein. Das zweite Kästchen wird danach automatisch ausgefüllt.
Private IP	Geben Sie die private IP-Adresse des internen Hosts an, der den Dienst anbietet. Falls Sie **Bereich** als Portumleitungsmodus wählen, sehen Sie in diesem Feld zwei Kästchen. Geben Sie im ersten Kästchen eine komplette IP-Adresse ein (als Anfangspunkt) und die vierte Zifferngruppe im zweiten Kästchen (als Endpunkt).
Privater Port	Geben Sie die private Portnummer des Dienstes an, den der interne Host anbietet.
Aktiv	Markieren Sie dieses Kästchen, um die definierte Port-Zuordnung zu aktivieren.

Beachten Sie, dass der Router eigene Dienste (Server) wie Telnet, HTTP und FTP hat. Da diese Dienste (Server) immer die gleichen Portnummern verwenden, kann es notwendig sein, die Portnummern des Routers zu ändern, um Konflikte zu vermeiden.

Das Router-Menü beispielsweise verwendet den Standardport 80, was einen Konflikt mit dem Webserver im lokalen Netzwerk (http://192.168.1.13:80) verursachen kann. **Ändern Sie daher den HTTP-Port des Routers auf einen anderen Port als den Standardport 80**, um einen Konflikt zu vermeiden, z.B. auf 8080. Dies kann unter **Systemmanagement >>Systemverwaltung** eingestellt werden. Danach haben Sie über Port 8080 Zugriff auf das Administrationsmenü (z.B. http://192.168.1.1:8080), nicht mehr über Port 80.

Systemmanagement >> Verwaltung

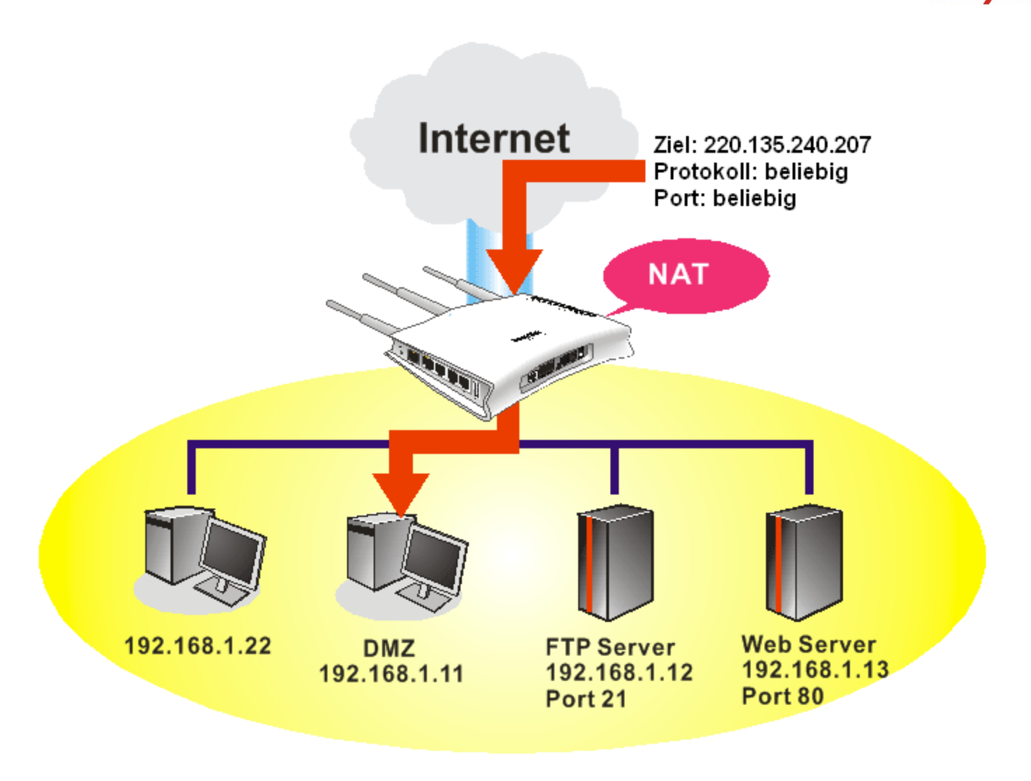
Systemverwaltung

Zugangsverwaltung			Port-Einstellungen verwalten		
☑ Management aus dem Internet erlauben			◉ benutzerdefinierte Ports		○ Standard-Ports
☐ FTP-Server			Telnet-Port	23	(Standard: 23)
☑ HTTP-Server			HTTP-Port	80	(Standard: 80)
☑ HTTPS-Server			HTTPS-Port	443	(Standard: 443)
☑ Telnet-Server			FTP-Port	21	(Standard: 21)
☐ SSH-Server			SSH-Port	22	(Standard: 22)
☑ Router ignoriert PING aus dem Internet					
Zugangsberechtigung			**SNMP-Einstellungen**		
Nr.	IP-Adresse	Subnetz-Maske	☐ SNMP aktiv		
1			Get Community	public	
2			Set Community	private	
3			IP des Host-Managers		
			Trap Community	public	
			Benachrichtigung an IP		
			Timeout für Trap	10	Sekunden

OK

4.3.2 DMZ-Host

Wie oben erwähnt, kann die **Portumleitung** eingehenden TCP-/UDP-Verkehr oder anderen Verkehr auf bestimmten Ports an die angegebene private IP-Adresse/Port des Hosts im LAN umleiten. Es ist jedoch zu beachten, dass andere IP-Protokolle wie z.B. die Protokolle 50 (ESP) und 51 (AH) nicht auf einem festen Port kommunizieren. Der Vigor-Router bietet eine **DMZ-Host**-Funktion, die sämtliche unangeforderte Daten auf beliebigen Protokollen einem einzigen Host im LAN zuordnet. Normales Web-Surfen und andere Internet-Aktivitäten anderer Clients funktionieren weiterhin ohne unangemessene Unterbrechung. **DMZ-Host** ermöglicht einem definierten internen Benutzer, dem Internet vollständig ausgesetzt zu sein, was für gewisse Anwendungen wie Netmeeting oder Internet-Spiele usw. notwendig sein mag.

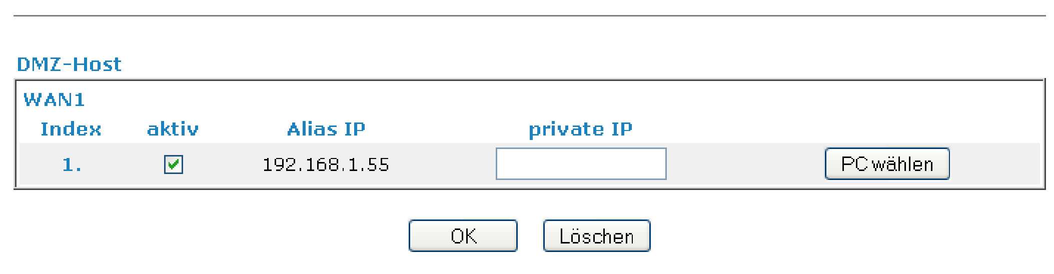


Die Sicherheitseigenschaften von NAT werden umgangen, wenn Sie einen DMZ-Host einrichten. Wir empfehlen Ihnen daher, zusätzliche Filterregeln oder eine zweite Firewall zu konfigurieren.

Klicken Sie auf **DMZ-Host**, um die folgende Seite zu öffnen:



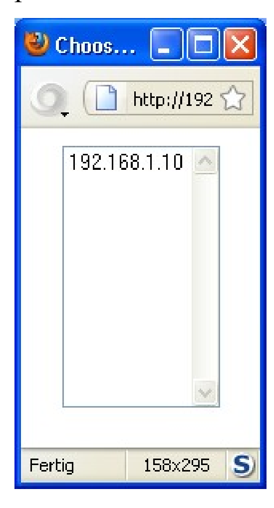
Falls Sie zuvor einen **WAN-Alias** für den **PPPoE/PPPoA** oder **MPoA**-Modus eingerichtet haben, finden Sie diesen unter **Alias IP** zur Auswahl.



Aktiv Markieren Sie dieses Kästchen, um die DMZ-Host-Funktion zu aktivieren.

Private IP Geben Sie die private IP-Adresse des DMZ-Hosts ein oder klicken Sie auf "PC wählen", um eine IP-Adresse zu wählen.

PC wählen Wenn Sie auf diese Taste klicken, öffnet sich automatisch das unten abgebildete Fenster. Das Fenster enthält eine Liste privater IP-Adressen aller Hosts in Ihrem LAN. Bestimmen Sie eine private IP-Adresse aus der Liste als DMZ-Host.



Nachdem Sie im oben gezeigten Dialog eine private IP gewählt haben, wird die IP-Adresse im folgenden Fenster angezeigt. Klicken Sie auf **OK**, um diese Einstellung zu speichern.

4.3.3 Offene Ports

Offene Ports ermöglicht Ihnen, einen Portbereich für den Verkehr besonderer Anwendungen zu öffnen.

Bestimmte Ports müssen beispielsweise für P2P-Anwendungen (BT, KaZaA, Gnutella, WinMX, eMule usw.), Webcam usw. geöffnet werden. Sorgen Sie dafür, dass die betreffende Anwendung immer auf dem neuesten Stand ist, um Angriffe auf eventuelle Sicherheitslücken zu vermeiden.

Klicken Sie auf **Offene Ports**, um die folgende Seite zu öffnen:

NAT >> Offene Ports

Einstellungen offener Ports | Auf Werkseinstellungen zurücksetzen |

Index	Bezeichnung	Alias IP	lokale IP-Adresse	Status
1.				x
2.				x
3.				x
4.				x
5.				x
6.				x
7.				x
8.				x
9.				x
10.				x

<< 1-10 | 11-20 >> Weiter >>

Index Geben Sie die relative Nummer eines bestimmten Eintrags an, für den Sie einen Dienst auf einem lokalen Host anbieten möchten. Klicken Sie auf die entsprechende Indexnummer, um den Eintrag zu bearbeiten oder zu löschen.

Bezeichnung Geben Sie die Bezeichnung des definierten Netzwerkdienstes an.

Lokale IP-Adresse Private IP-Adresse des lokalen Hosts anzeigen, der den Dienst anbietet.

Status Status des entsprechenden Eintrags anzeigen. X oder V steht für **Inaktiv** bzw. **Aktiv**.

Um Porteinstellungen hinzuzufügen oder zu bearbeiten, klicken Sie auf eine der Indexnummern auf der Seite. Die Konfigurationsseite für den Indexeintrag erscheint. In jedem Indexeintrag können Sie **10** Portbereiche für verschiedene Dienste angeben.

NAT >> Offene Ports >> Konfiguration

Index-Nr. 1

☑ aktiv

Bezeichnung P2P

lokaler Computer 192.168.1.10 PC wählen

	Protokoll	Start-Port	End-Port		Protokoll	Start-Port	End-Port
1.	TCP	4500	4700	6.	—	0	0
2.	UDP	4500	4700	7.	—	0	0
3.	—	0	0	8.	—	0	0
4.	—	0	0	9.	—	0	0
5.	—	0	0	10.	—	0	0

OK Löschen Abbrechen

Aktiv Markieren Sie dieses Kästchen, um diesen Eintrag zu aktivieren.

Bezeichnung Geben Sie die Bezeichnung der definierten Netzwerkanwendung/des definierten Netzwerkdienstes an.

WAN-Schnittstelle Geben Sie die WAN-Schnittstelle an, die für diesen Eintrag verwendet werden soll.

Lokaler Computer Geben Sie die private IP-Adresse des lokalen Hosts ein oder klicken Sie auf **PC wählen**, um eine IP-Adresse zu wählen.

PC wählen Wenn Sie auf diese Taste klicken, öffnet sich automatisch ein Fenster mit einer Liste privater IP-Adressen von lokalen Hosts. Wählen Sie die entsprechende IP-Adresse des lokalen Hosts aus der Liste.

Protokoll Wählen Sie das Protokoll für die Transportschicht. Zur Auswahl stehen **TCP**, **UDP** oder **-----** (keines).

Start-Port Geben Sie die Start-Portnummer des Dienstes an, den der interne Host anbietet.

End-Port Geben Sie die End-Portnummer des Dienstes an, den der interne Host anbietet.

4.4 Firewall

4.4.1 Firewall-Grundlagen

Der zunehmende Bedarf nach Bandbreite für Multimedia, interaktive Anwendungen und Fernunterricht steht verschiedenen Sicherheitsbedenken gegenüber. Die Firewall des Vigor-Routers ermöglicht Ihnen, Ihr lokales Netzwerk vor Angriffen Unbefugter zu schützen. Die Firewall kann auch die Nutzung des Internet durch Benutzer im lokalen Netzwerk beschränken. Außerdem ist es möglich, gewisse Pakete zu verwerfen, die den Router veranlassen würden, eine unerwünschte Verbindung nach außen aufzubauen.

Eigenschaften der Firewall

Die folgenden Firewall-Eigenschaften schützen die Benutzer im LAN:

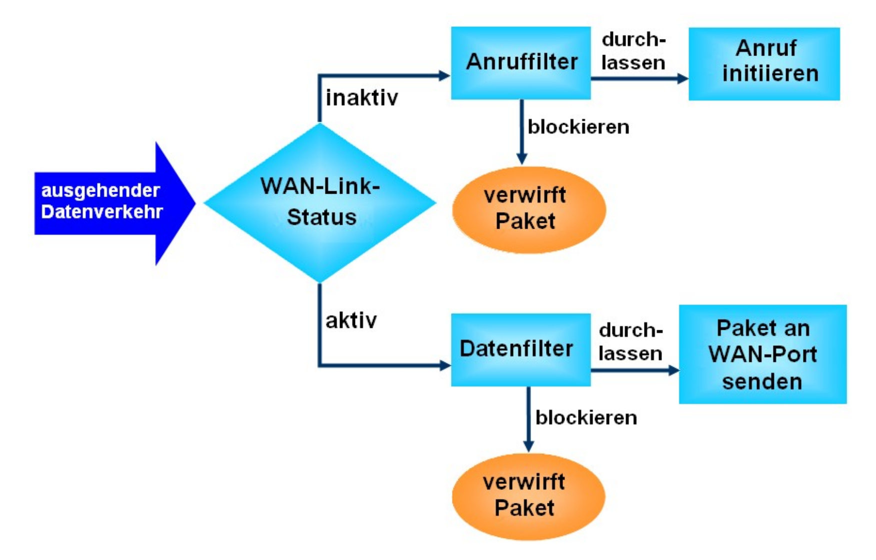
- Benutzerabhängige IP-Filter (Anruffilter/Datenfilter)
- SPI (Stateful Packet Inspection) kontrolliert Pakete und blockiert nicht angeforderte eingehende Daten.
- Optionaler Schutz vor DoS/DDoS-Angriffen

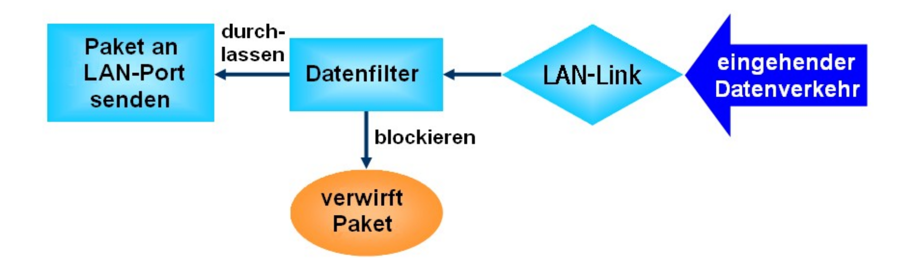
IP-Filter

Je nachdem, ob eine Internet-Verbindung existiert oder nicht, d.h. je nachdem, ob die WAN-Verbindung aktiv ist oder nicht, unterscheidet die IP-Filterarchitektur zwei Arten von Filtern: **Anruffilter** und **Datenfilter**.

- **Anruffilter -** Falls keine Verbindung zum Internet besteht, wird der **Anruffilter** auf den ausgehenden Verkehr angewendet. Er überprüft die Pakete gemäß den Filterregeln. Zulässige Pakete werden durchgelassen. Der Router veranlasst daraufhin einen **Anruf**, um die Internet-Verbindung aufzubauen und das Paket über das Internet zu versenden.
- **Datenfilter** - Falls eine Verbindung zum Internet besteht, wird der **Datenfilter** auf den ein- und ausgehenden Verkehr angewendet. Er überprüft die Pakete gemäß den Filterregeln. Zulässige Pakete werden durch den Router durchgelassen.

Die folgenden Flussdiagramme veranschaulichen, wie der Router mit ein- und ausgehendem Verkehr umgeht.





Stateful Packet Inspection (SPI)

Stateful Inspection ist eine Firewall-Architektur, die auf der Netzwerkschicht implementiert ist. Im Gegensatz zur herkömmlichen statischen Paketfilterung, welche ein Paket anhand der Informationen im Header analysiert, baut Stateful Inspection eine Statustabelle auf, um alle Verbindungen zu kontrollieren, welche sämtliche Schnittstellen der Firewall passieren, und sorgt dafür, dass diese gültig sind. Die Stateful Firewall des Vigor-Routers kontrolliert somit nicht nur die Header-Information, sondern auch den Verbindungsstatus.

DoS-Abwehr

Die Funktionalität der **DoS-Abwehr** ermöglicht die Erkennung und Entschärfung von DoS-Angriffen. Die Angriffe können entweder durch Überflutung (Flooding) stattfinden oder direkt auf Schwachstellen abzielen. Der Überflutungsansatz versucht, Ihre Systemressourcen komplett in Anspruch zu nehmen, während die eigentlichen Angriffe den Zweck verfolgen, die Schwachstellen des Protokolls oder des Betriebssystems auszunutzen.

Die **DoS-Abwehr**funktion ermöglicht dem Vigor-Router, jedes eingehende Paket anhand der Angriffssignaturdatenbank zu analysieren. Jedes bösartige Paket, das sich vervielfältigen könnte, um den Host im sicheren LAN lahmzulegen, wird grundsätzlich blockiert. Sofern Sie einen Syslog-Server eingerichtet haben, wird außerdem eine Syslog-Meldung versandt.

Der Vigor-Router beobachtet auch den Verkehr. Ungewöhnliche Verkehrsflüsse, welche vorher festgelegte Parameter wie die Anzahl der Schwellenwerte überschreiten, werden als Angriff gekennzeichnet. Der Vigor-Router aktiviert daraufhin seinen Abwehrmechanismus, um den Angriff in Echtzeit unschädlich zu machen.

Nachfolgend sind die Angriffsarten aufgeführt, die von der DoS/DDoS-Verteidigungsfunktion erkannt werden können:

1. SYN Flood Angriff
2. UDP Flood Angriff
3. ICMP Flood Angriff
4. Port Scan Angriff
5. IP Options
6. Land-Angriff
7. Smurf-Angriff
8. Trace Route
9. SYN Fragmente
10. Fraggle-Angriff
11. TCP Flag Scan
12. Teardrop-Angriff
13. Ping of Death Angriff
14. ICMP Fragmente
15. Unbekanntes Protokoll

4.4.2 Basiskonfiguration

Unter **Basiskonfiguration** können Sie die IP-Filtereinstellungen und andere allgemeine Optionen konfigurieren. **Anruffilter** und **Datenfilter** können hier aktiviert oder deaktiviert werden. Unter gewissen Voraussetzungen können Ihre Filter-Sätze so kombiniert werden, dass diese nacheinander abgearbeitet werden. Hier müssen Sie lediglich den **Ersten Filter-Satz** einstellen. Außerdem können Sie die **Log Flag**-Einstellungen konfigurieren, den **Filter auf alle eingehenden VPN-Verbindungen anwenden** und **Fragmentierte UDP-Pakete akzeptieren**.

Wählen Sie **Firewall** und klicken Sie auf **Basiskonfiguration**, um die Seite mit den grundlegenden Einstellungen zu öffnen.

Firewall >> Basiskonfiguration

Basiskonfiguration

Anruffilter	◉ aktiv ○ inaktiv	Erster Filter-Satz	Satz 1
Datenfilter	◉ aktiv ○ inaktiv	Erster Filter-Satz	Satz 2

Aktionen für Standardregeln:

Anwendungen	Aktion/Profil	Syslog
Basisfilter	Pakete durchlassen	☐
IM/P2P Filter	Aus	☐
Inhaltsbezogener URL-Filter	Aus	☐
Web Content Filter	Aus	☐

Erweiterte Einstellungen [Ändern]

☑ Fragmentierte UDP- oder ICMP-Pakete akzeptieren (für einige Online-Spiele, z.B. CS)

[OK] [Abbrechen]

Anruffilter — Markieren Sie **Aktiv**, um die Anruffilterfunktion zu aktivieren. Wählen Sie den ersten Filter-Satz für den Anruffilter.

Datenfilter — Markieren Sie **Aktiv**, um die Datenfilterfunktion zu aktivieren. Wählen Sie den ersten Filter-Satz für den Datenfilter.

Basisfilter — Wählen Sie für die Pakete, die den Filterregeln nicht entsprechen, **Durchlassen** oder **Blockieren**.

Pakete durchlassen
Pakete durchlassen
Pakete blockieren

IM/P2P-Filter — Wählen Sie für die umfassende Blockierung von IM/P2P-Anwendungen ein CSM-Profil. Alle Hosts im LAN unterliegen dem im hier gewählten CSM-Profil konfigurierten Standard. Einzelheiten werden im Abschnitt über die Einrichtung des CSM-Profils erläutert. Zur Fehlersuche können Sie die IM/P2P-bezogenen Vorgänge aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 3.14.4 **Syslog/Mail-Alarm**.

Inhaltsbezogener — Wählen Sie eine der Profileinstellungen für den **inhaltsbezogenen**

URL-Filter

URL-Filter (erstellt in **CSM>> Inhaltsbezogener URL-Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> URL-Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum URL-Filter aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 3.14.4 **Syslog/Mail-Alarm**.

Inhaltsbezogener Web-Filter

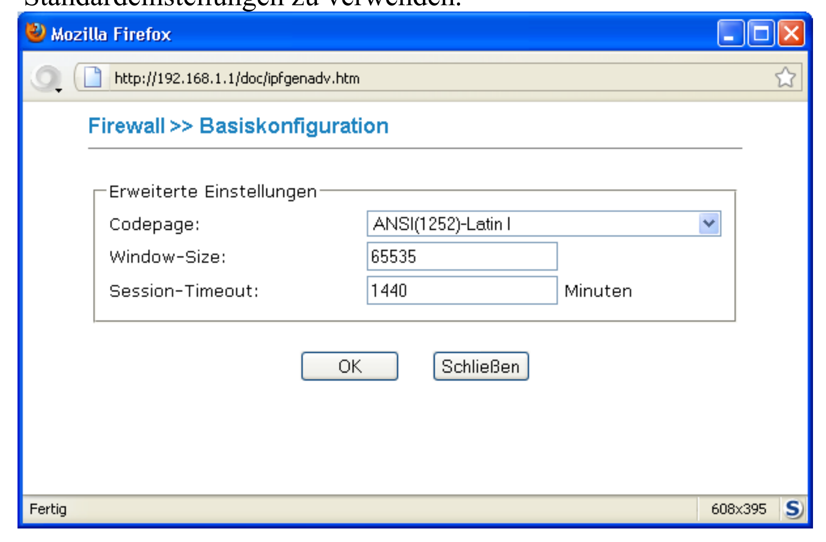
Wählen Sie eine der Profileinstellungen für den **inhaltsbezogenen Web-Filter** (erstellt in **CSM>> Inhaltsbezogener Web-Filter**), welche dieser Router anwenden soll. Richten Sie zunächst mindestens ein Profil zur Auswahl unter **CSM>> Inhaltsbezogener Web-Filter** ein. Zur Fehlersuche können Sie die Vorgänge zum **inhaltsbezogenen Web-Filter** aufzeichnen, indem Sie die Log-Funktion aktivieren. Die Meldungen werden an den Syslog-Server gesandt. Zu Einzelheiten sehen Sie bitte Abschnitt 3.14.4 **Syslog/Mail-Alarm**.

Syslog

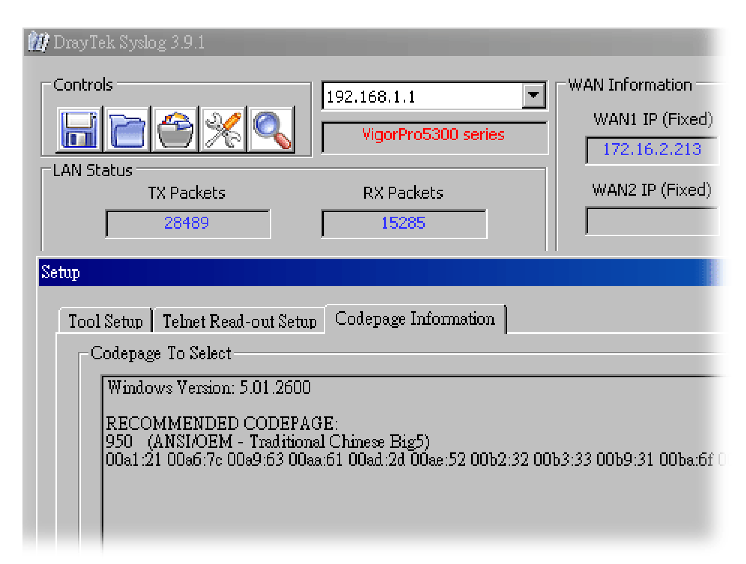
Zur Fehlersuche können Sie das Filter-Log und/oder das CSM-Log durch Anhaken des Kästchens aktivieren. Das Log wird im DrayTek Syslog-Fenster angezeigt.

Erweiterte Einstellungen

Klicken Sie auf **Bearbeiten**, um das folgende Fenster zu öffnen. Es wird jedoch **dringend empfohlen**, hier die Standardeinstellungen zu verwenden.



Codepage - Diese Funktion wird verwendet, um die Zeichen verschiedener Sprachen zu vergleichen. Die Auswahl der korrekten Codepage ermöglicht dem System, die Daten der URL in korrekte ASCII-Zeichen umzuwandeln und die Treffsicherheit des inhaltsbezogenen URL-Filters zu verbessern. Die Standardeinstellung ist ANSI 1252 Latin I. Falls Sie keine Codepage wählen, werden URLs nicht umgewandelt. Bitte wählen Sie eine Codepage aus der Dropdown-Liste.
Falls Sie sich nicht sicher sind, welche Codepage zu wählen ist, öffnen Sie bitte Syslog. Die empfohlene Codepage ist im Reiter Codepage-Information des Konfigurationsdialogs aufgeführt.



Window-Size – Bestimmt die Größe des TCP-Protokolls (0~65535). Je größer der Wert ist, desto besser wird die Leistung sein. Falls das Netzwerk jedoch nicht stabil ist, ist ein kleiner Wert geeigneter.
Session-Timeout – Die Einstellung einer maximalen Dauer für Sitzungen ermöglicht die bestmögliche Nutzung der Netzwerkressourcen. Der Queue-Timeout gilt lediglich für das TCP-Protokoll, der Session-Timeout wird für den Datenfluss konfiguriert, welcher der Firewall-Regel entspricht.

Einige Online-Spiele (z.B. Half Life) verwenden eine Vielzahl von fragmentierten UDP-Paketen, um Game-Daten zu übermitteln. Als sichere Firewall verwirft der Vigor-Router diese fragmentierten Pakete normalerweise, um Angriffe zu vermeiden, es sei denn, Sie aktivieren **Fragmentierte UDP- oder ICMP-Pakete akzeptieren**. Wenn dieses Kästchen angehakt ist, können Sie solche Online-Spiele spielen. Falls Sicherheitsbedenken schwerer wiegen, aktivieren Sie **Fragmentierte UDP- oder ICMP-Pakete akzeptieren** lieber nicht.

4.4.3 Filtereinstellung

Klicken Sie auf **Firewall** und wählen Sie **Filtereinstellung**, um die Konfigurationsseite zu öffnen.

Firewall >> Filtereinstellung

Filtereinstellung | Auf Werkseinstellungen zurücksetzen |

Satz	Bezeichnung	Satz	Bezeichnung
1.	Default Call Filter	7.	
2.	Default Data Filter	8.	
3.		9.	
4.		10.	
5.		11.	
6.		12.	

Um einen Filter zu bearbeiten oder hinzuzufügen, klicken Sie auf die entsprechende Satznummer. Die folgende Seite erscheint. Jeder Filter-Satz kann bis zu sieben Regeln enthalten. Klicken Sie auf die Taste mit der Regelnummer, um die entsprechende Regel zu bearbeiten. Markieren Sie das Kästchen **Aktiv**, um die Regel zu aktivieren.

Filterregel Klicken Sie auf eine der Nummern (1 ~ 7), um die entsprechende Filterregel zu bearbeiten. Die Web-Seite Filterregeln ändern erscheint. Die folgende Seite enthält detaillierte Informationen.

Aktiv Filterregel aktivieren oder deaktivieren.

Bezeichnung Geben Sie eine Bezeichnung für den Filter-Satz ein. Die maximale Länge beträgt 23 Zeichen.

Aufwerten/Abwerten Klicken Sie auf **Nach oben** oder **Nach unten**, um die Reihenfolge der Filterregeln zu ändern.

Nächster Filter-Satz Setzen Sie den Link auf den nächsten Filter-Satz, der nach dem aktuellen Filter ausgeführt werden soll. Vermeiden Sie Ketten mit zu vielen Filter-Sätzen.

Um eine **Filterregel** zu bearbeiten, klicken Sie auf die Indexnummer der **Filterregel**, wodurch Sie auf die Konfigurationsseite für die **Filterregel** gelangen.

Firewall >> Filtereinstellung >> Filterregeln ändern

Filter-Satz 1 Regel 1

☑ Filterregel aktiv

Bezeichnung:	Block NetBios	
Index (1-15) aus der Verbindungstimer Konfiguration:	, , ,	
Richtung:	LAN -> WAN	
Quell-IP:	Any	Bearbeiten
Ziel-IP:	Any	Bearbeiten
Servicetyp:	TCP/UDP, Port: from 137~139 to undefined	Bearbeiten
Regel bezieht sich auf:	alle Datenpakete	
Anwendungen	**Aktion/Profil**	**SysLog**
Filter:	sofort blockieren	☐
Weiterleiten an Filter-Satz:	aus	
IM/P2P Filter:	aus	☐
Inhaltsbezogener URL-Filter	aus	☐
Web Content Filter	aus	☐
Erweiterte Einstellungen	Bearbeiten	

OK Löschen Abbrechen

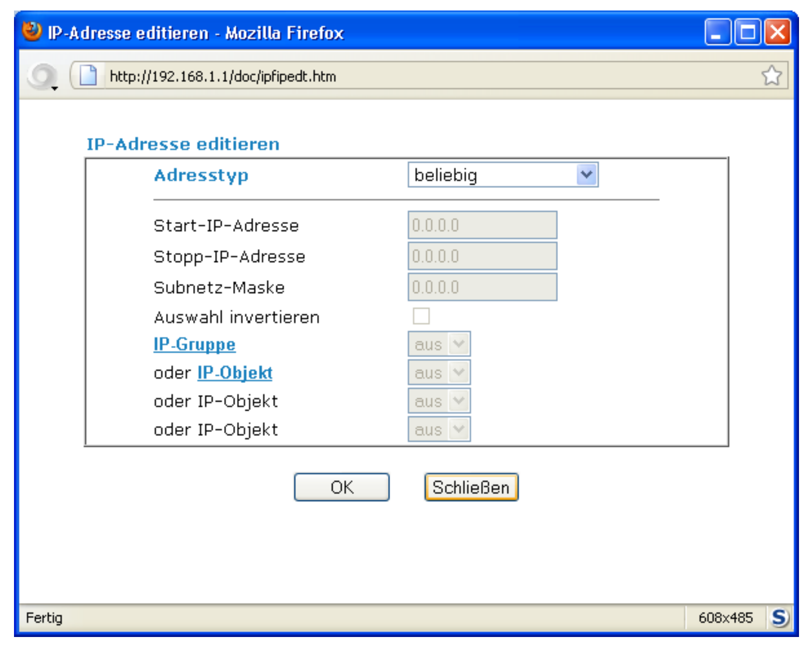
Filterregel aktiv Markieren Sie dieses Kästchen, um die Filterregel zu aktivieren.

Beschreibung Geben Sie eine Bezeichnung für den Filter-Satz ein. Die maximale Länge beträgt 14 Zeichen.

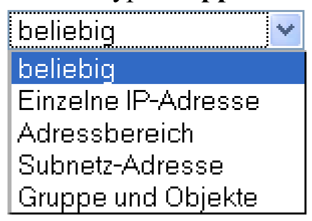
Index (1-15) Sie können die LAN-PCs so konfigurieren, dass sie lediglich in gewissen Zeitabschnitten in Betrieb sind. Sie können bis zu vier der 15 vordefinierten Timer unter **Anwendungen** >> **Timer** wählen. Per Standardeinstellung ist dieses Feld leer, und die Funktion ist ständig in Betrieb.

Richtung Stellen Sie die Paketflussrichtung ein (LAN->WAN/WAN->LAN). Dies gilt nur für den **Datenfilter**. Beim **Anruffilter** gilt diese Einstellung nicht, da sich dieser lediglich auf den ausgehenden Verkehr bezieht.

Quell-/Ziel-IP Klicken Sie auf **Bearbeiten**, um in den folgenden Dialog zu gelangen, in dem Sie die Quell-/Ziel-IP oder IP-Bereiche wählen können.



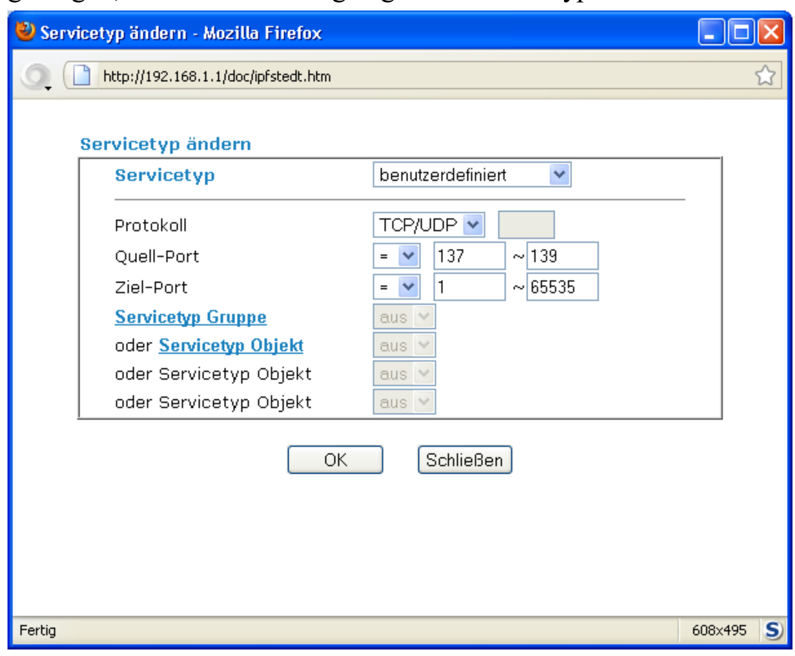
Um die IP-Adresse manuell einzustellen, wählen Sie bitte als Adresstyp **Beliebige Adresse/Einzelne Adresse/Adressbereich/Subnetz-Adresse** und geben sie in diesem Dialog ein. Falls Sie außerdem den IP-Bereich bestimmter Gruppen oder Objekte verwenden möchten, wählen Sie bitte als Addresstyp **Gruppen und Objekte**.



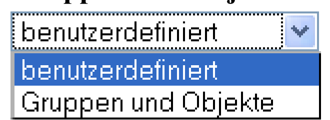
Aus der Dropdown-Liste **IP-Gruppe** wählen Sie diejenige, die Sie anwenden möchten. Alternativ können Sie die Dropdown-Liste **IP-Objekt** benutzen, um das gewünschte Objekt zu wählen.

Servicetyp

Klicken Sie auf **Bearbeiten**, um in den folgenden Dialog zu gelangen, in dem Sie einen geeigneten Servicetyp wählen können.



Um den Servicetyp manuell einzustellen, wählen Sie bitte **Benutzerdefiniert** als Servicetyp und geben ihn in diesem Dialog ein. Falls Sie außerdem den Servicetyp bestimmter Gruppen oder Objekte verwenden möchten, wählen Sie bitte als Servicetyp **Gruppen und Objekte**.



Protokoll - Geben Sie das/die Protokoll(e) an, auf welche(s) diese Filterregel anzuwenden ist.

Quell-/Ziel-Port -

(=) – Identische erste und letzte Werte weisen auf einen einzelnen Port hin; unterschiedliche erste und letzte Werte weisen auf einen Portbereich hin, der für diesen Servicetyp verfügbar ist.

(!=) – Identische erste und letzte Werte weisen auf alle Ports außer dem hier angegebenen Port hin; unterschiedliche erste und letzte Werte weisen darauf hin, dass alle Ports außer dem hier angegebenen Bereich für diese Servicetyp verfügbar sind.

(>) – Die Portnummer, die größer als dieser Wert ist, ist verfügbar.

(<) – Die Portnummer, die kleiner als dieser Wert ist, ist für dieses Profil verfügbar.

Servicetyp Gruppe/Objekt - Verwenden Sie die Dropdown-Liste, um Ihre Auswahl zu treffen.

Fragmente

Bestimmen Sie die Aktion für fragmentierte Pakete. Dies gilt lediglich für den **Datenfilter**.

Alle Datenpakete - Keine Aktion für fragmentierte Pakete.

Alle nicht fragmentierten Pakete - Regel auf nicht fragmentierte Pakete anwenden.

Alle fragmentierten Pakete - Regel auf fragmentierte Pakete anwenden.

Alle Fragmente ohne Header - Regel nur auf Pakete anwenden, die zu kurz sind, um einen vollständigen Header zu enthalten.

Basisfilter

Gibt die durchzuführende Aktion an, wenn Pakete der Regel entsprechen.

Sofort blockieren - Pakete, die mit der Regel übereinstimmen, werden sofort verworfen.

Sofort durchlassen - Pakete, die mit der Regel übereinstimmen, werden sofort durchgelassen.

Blockieren, falls keine weitere Übereinstimmung - Pakete, die mit der Regel übereinstimmen und mit keinen weiteren Regeln übereinstimmen, werden verworfen.

Durchlassen, falls keine weitere Übereinstimmung - Pakete, die mit der Regel übereinstimmen und mit keinen weiteren Regeln übereinstimmen, werden durchgelassen.

Weiterleiten an Filter-Satz

Falls das Paket der Filterregel entspricht, leitet die nächste Filterregel das Paket zum angegebenen Filter-Satz weiter. Wählen Sie die nächste Filterregel aus dem Dropdown-Menü. Vergessen Sie nicht, dass der Router die angegebene Filterregel ständig anwenden wird und nicht mehr zur vorherigen Filterregel zurückkehren wird.

CSM

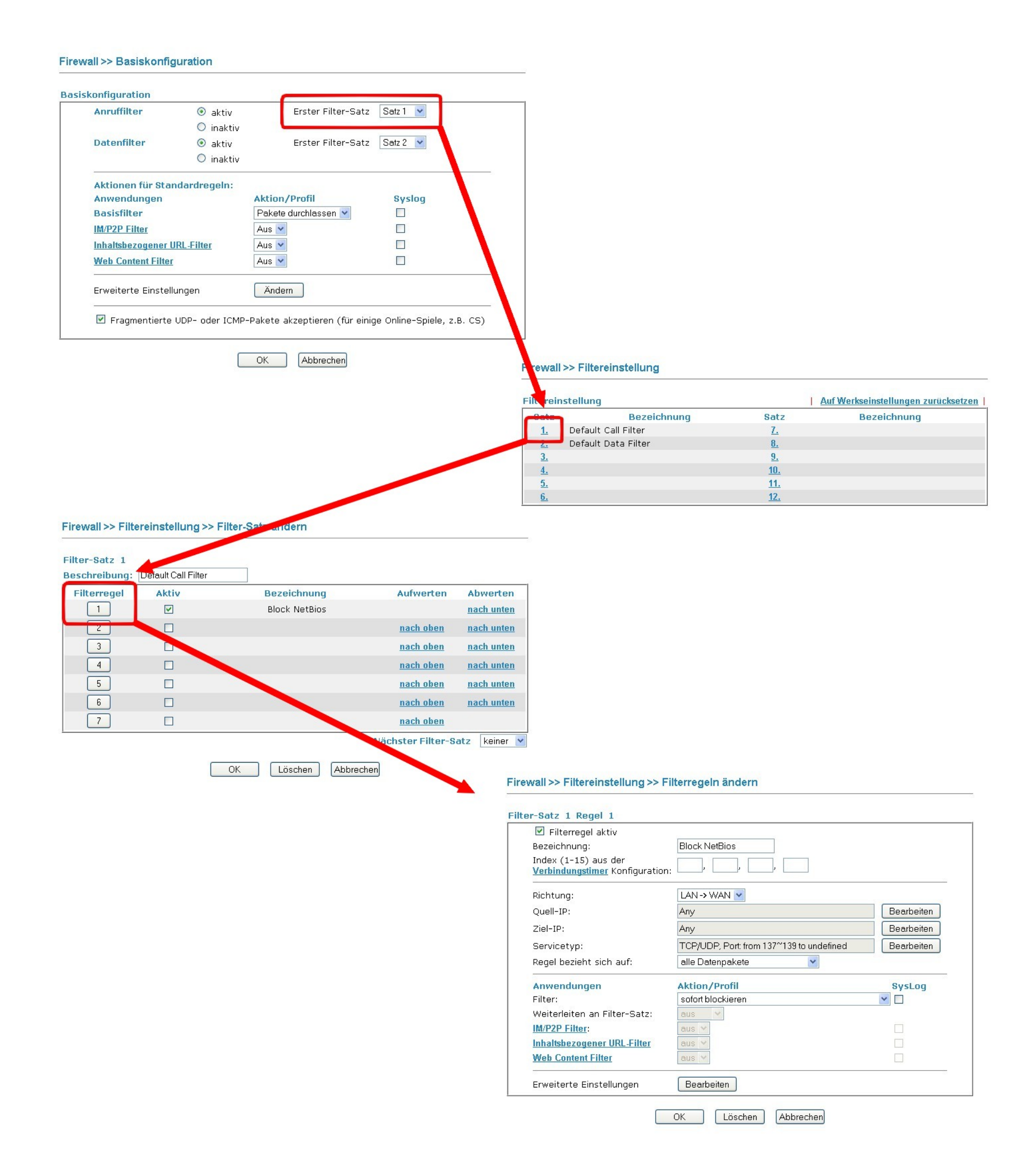
Alle Pakete/Verbindungen im Bereich der oben konfigurierten

Bedingungen müssen dem Standard entsprechen, der in dem hier gewählten CSM-Profil konfiguriert wurde. Einzelheiten werden im Abschnitt über die Einrichtung des CSM-Profils erläutert.

SysLog Zur Fehlersuche können Sie hier das Filter-Log und/oder das CSM-Log aktivieren. Markieren Sie das entsprechende Kästchen, um die Log-Funktion zu aktivieren. Daraufhin wird das Filter-Log und/oder CSM-Log im DrayTek Syslog-Fenster angezeigt.

Beispiel

Wie bereits erwähnt, wird der gesamte Verkehr mit Hilfe von zwei IP-Filtern aufgeteilt und vermittelt: Anruffilter oder Datenfilter. Sie können unter **Filtereinstellung** bis zu zwölf Anruffilter und Datenfilter einrichten und diese sogar seriell kombinieren. Jeder Filter-Satz besteht aus sieben Filterregeln, die näher definiert werden können. Danach können Sie in der **Basiskonfiguration** einen Satz als zuerst anzuwendenden Anruffilter oder Datenfilter bestimmen.



4.4.4 DoS-Abwehr

Als Subfunktionalität der IP-Filter/Firewall gibt es 15 Arten von Erkennungs-/Abwehrfunktionen in der Konfiguration der **DoS-Abwehr**. Die DoS-Abwehrfunktionalität ist standardmäßig deaktiviert.

Wählen Sie **Firewall** und klicken auf **DoS-Abwehr**, um die Konfigurationsseite zu öffnen.

Firewall >> DoS-Abwehr

DoS-Abwehr

☑ aktiv			
☐ Aktiviere SYN Flood Abwehr	Schwellenwert	50	Pakete / Sek.
	Zeitlimit	10	Sek.
☐ Aktiviere UDP Flood Abwehr	Schwellenwert	150	Pakete / Sek.
	Zeitlimit	10	Sek.
☐ Aktiviere ICMP Flood Abwehr	Schwellenwert	50	Pakete / Sek.
	Zeitlimit	10	Sek.
☐ Aktiviere Port Scan Abwehr	Schwellenwert	150	Pakete / Sek.
☐ IP Options blockieren	☐ TCP Flag Scan blockieren		
☐ Land blockieren	☐ Tear Drop blockieren		
☐ Smurf blockieren	☐ Ping of Death blockieren		
☐ Trace Route blockieren	☐ ICMP Fragment blockieren		
☐ SYN Fragmente blockieren	☐ unbekannte Protokolle blockieren		
☐ Fraggle Attack blockieren			

Aktivieren Sie die DoS-Abwehrmechanismen, um sich vor Hackern und Crackern zu schützen.

OK | Alles löschen | Abbrechen

Aktiv — Markieren Sie das Kästchen, um die DoS-Abwehrfunktionalität zu aktivieren.

Aktiviere SYN Flood Abwehr — Markieren Sie das Kästchen, um die SYN Flood Abwehrfunktion zu aktivieren. Sobald der Schwellenwert der TCP SYN Pakete aus dem Internet den definierten Wert überschreitet, beginnt der Vigor-Router, die folgenden TCP SYN Pakete, die über dem unter Timeout definierten Zeitraum liegen, zufällig zu verwerfen. Der Zweck dieser Vorgehensweise ist, zu vermeiden, dass die TCP SYN Pakete die begrenzten Ressourcen des Vigor-Routers ausschöpfen. Standardmäßig wird der Schwellenwert auf 50 Pakete pro Sekunde und der Timeout auf 10 Sekunden gesetzt.

Aktiviere UDP Flood Abwehr — Markieren Sie das Kästchen, um die UDP Flood Abwehrfunktion zu aktivieren. Sobald der Schwellenwert der UDP-Pakete aus dem Internet den definierten Wert überschreitet, beginnt der Vigor-Router, die folgenden UDP-Pakete, die über dem unter Timeout definierten Zeitraum liegen, zufällig zu verwerfen. Standardmäßig wird der Schwellenwert auf 150 Pakete pro Sekunde und der Timeout auf 10 Sekunden gesetzt.

Aktiviere ICMP Flood Abwehr	Markieren Sie das Kästchen, um die ICMP Flood Abwehrfunktion zu aktivieren. Ähnlich wie bei der UDP Flood Abwehrfunktion verwirft der Router daraufhin die aus dem Internet kommenden ICMP-Echo-Requests, sobald der Schwellenwert der ICMP-Pakete aus dem Internet den definierten Wert überschreitet. Standardmäßig werden der Schwellenwert auf 50 Pakete pro Sekunde und der Timeout auf 10 Sekunden gesetzt.
Aktiviere Port Scan Abwehr	Bei Port Scan Angriffen auf den Vigor-Router werden viele Pakete an viele Ports gesandt, um eine Antwort von bestimmten Diensten zu erhalten. Markieren Sie das Kästchen, um die Port Scan Erkennung zu aktivieren. Jedes Mal, wenn dieses bösartige Suchverhalten erkannt wird, was durch Überwachung des Port Scan Schwellenwertes geschieht, versendet der Vigor-Router eine Warnung. Standardmäßig beträgt der Schwellenwert des Vigor-Routers 150 Pakete pro Sekunde.
IP-Options blockieren	Markieren Sie das Kästchen, um die Funktion zum Blockieren von IP-Options zu aktivieren. Der Vigor-Router wird somit jegliche IP-Pakete mit IP-Option-Feld im Datagramm-Header ignorieren. Der Grund für die Beschränkung von IP-Options besteht darin, wichtige Informationen wie Sicherheits- und TCC-Parameter (geschlossene Benutzergruppe), eine Reihe von Internet-Adressen, Routing-Meldungen usw. nicht weiterzugeben. Ein Außenstehender könnte sonst Einzelheiten über Ihre privaten Netzwerke in Erfahrung bringen.
Land blockieren	Markieren Sie das Kästchen, damit der Vigor-Router Land-Attacken abwehrt. Die Land-Attacke verbindet die Technologie der SYN-Angriffe mit IP-Spoofing. Eine Land-Attacke findet statt, wenn ein Angreifer gefälschte SYN-Pakete, bei denen die Quell- und Zieladressen sowie die Portnummer identisch sind, an potentielle Opfer sendet.
Smurf blockieren	Markieren Sie das Kästchen, um die Funktion zum Blockieren von Smurf zu aktivieren. Der Vigor-Router wird daraufhin jegliche ICMP-Echo-Requests an die Broadcast-Adresse ignorieren.
Trace Route blockieren	Markieren Sie das Kästchen, damit der Vigor-Router keine Trace Route Pakete weiterleitet.
SYN Fragmente blockieren	Markieren Sie das Kästchen, um die Funktion zum Blockieren von SYN-Fragmenten zu aktivieren. Der Vigor-Router wird daraufhin jegliche Pakete verwerfen, bei denen das SYN-Flag gesetzt ist und die zusätzliche Bit-Fragmente haben.
Fraggle Attack blockieren	Markieren Sie das Kästchen, um die Funktion zum Blockieren von Fraggle-Attacken zu aktivieren. Jegliche aus dem Internet erhaltene UDP-Pakete an die Broadcast-Adresse werden blockiert.

Die Aktivierung der DoS/DDoS-Abwehrfunktionalität kann unter Umständen auch gültige Pakete blockieren. Wenn Sie zum Beispiel die Abwehr von Fraggle-Attacken aktivieren, werden alle aus dem Internet kommenden UDP-Pakete an die Broadcast-Adresse blockiert. Folglich können auch die RIP-Pakete aus dem Internet verworfen werden.

TCP Flag Scan blockieren
Markieren Sie das Kästchen, um die Funktion zum Blockieren von TCP Flag Scan zu aktivieren. Jegliche TCP-Pakete mit anormal gesetzten Flags werden verworfen. Diese Scan-Aktivitäten umfassen *Null Scan*, *FIN ohne ACK Scan*, *SYN FIN Scan*, *Xmas Scan* und *Full Xmas Scan*.

Tear Drop blockieren
Markieren Sie das Kästchen, um die Funktion zum Blockieren von Tear Drop zu aktivieren. Viele Rechner können abstürzen, wenn sie ICMP-Datagramme (Pakete) erhalten, welche die maximale Länge überschreiten. Um diese Art von Angriffen zu vermeiden, hat der Vigor-Router die Fähigkeit, fragmentierte ICMP-Pakete mit einer Länge von mehr als 1.024 Oktetten zu verwerfen.

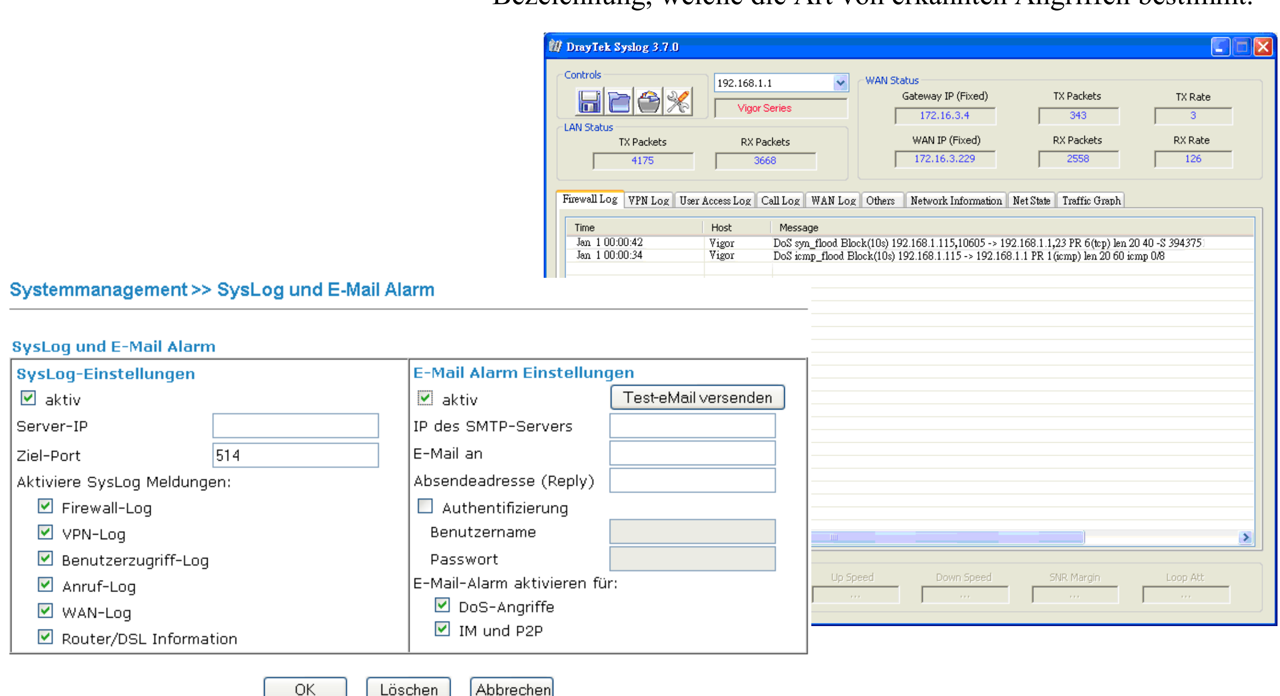
Ping of Death blockieren
Markieren Sie das Kästchen, um die Funktion zum Blockieren von Ping of Death zu aktivieren. Bei dieser Art von Angriffen sendet der Angreifer überlappende Pakete an die Ziel-Hosts, damit diese hängen bleiben, wenn sie die Pakete wieder zusammensetzen. Der Vigor-Router wird jegliche Pakete blockieren, bei welchen diese Angriffsaktivität festgestellt wird.

ICMP Fragment blockieren
Markieren Sie das Kästchen, um die Blockierfunktion für ICMP-Fragmente zu aktivieren.

Unbekannte Protokolle blockieren
Markieren Sie das Kästchen, um die Funktion zum Blockieren von unbekannten Protokollen zu aktivieren. Einzelne IP-Pakete haben im Datagramm-Header ein Protokollfeld, in dem der Protokolltyp angegeben wird. Protokolltypen über 100 sind jedoch reserviert und bis jetzt undefiniert. Daher sollte der Router in der Lage sein, diese Art von Paketen zu erkennen und abzulehnen.

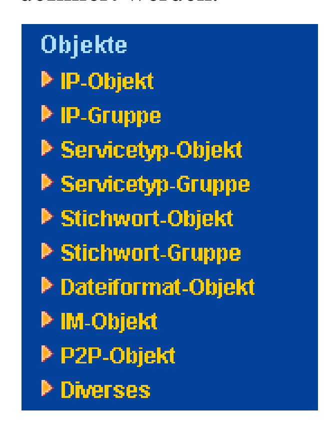
Warnmeldungen
Die Syslog-Funktion ermöglicht die Annahme von Meldungen vom Vigor-Router. Der Benutzer als Syslog-Server erhält die Meldungen vom Vigor-Router, dem Syslog-Client.

Sämtliche mit der **DoS-Abwehr** zusammenhängenden Warnmeldungen werden an den Benutzer gesandt, der sie über den Syslog-Daemon kontrollieren kann. Suchen Sie in der Meldung nach dem Schlüsselwort **DoS**, gefolgt von einer Bezeichnung, welche die Art von erkannten Angriffen bestimmt.



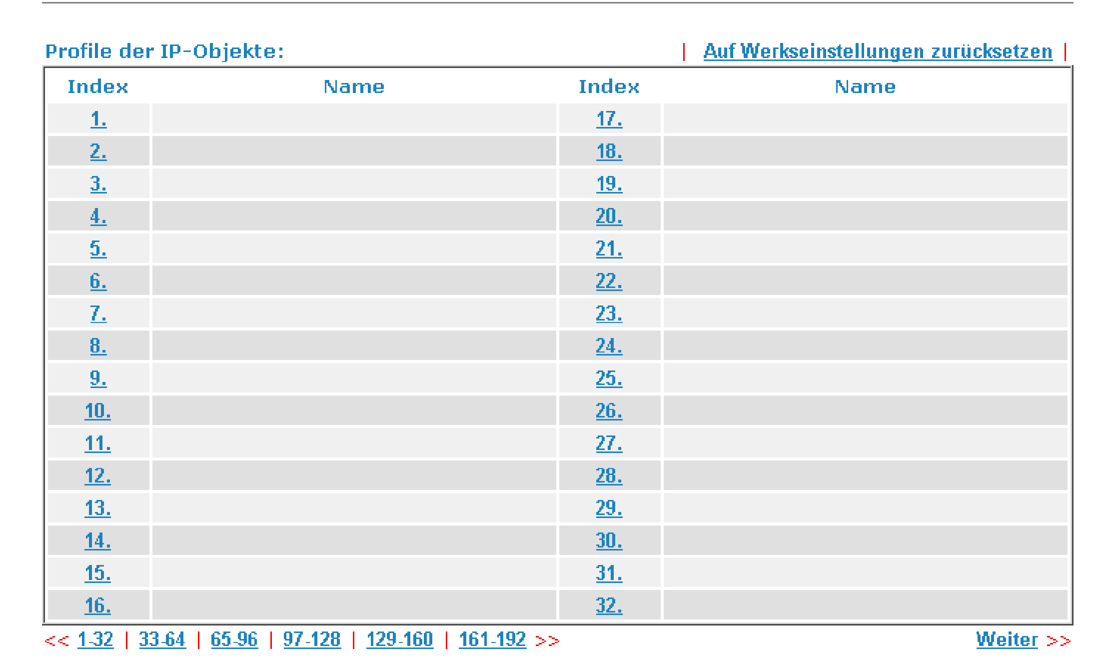
4.5 Objekte

IP-Bereiche und Port-Bereiche, auf welche eine bestimmte Router-Konfiguration angewendet werden soll, können als ***Objekte*** definiert werden, die zwecks vereinfachter Handhabung als ***Gruppen*** zusammengefasst werden können. Daraufhin steht das entsprechende Objekt/die Gruppe für die Anwendung der Einstellungen zur Auswahl. Es können beispielsweise alle IPs einer Abteilung als IP-Objekt (IP-Adressbereich) definiert werden.



4.5.1 IP-Objekt

Sie können bis zu 192 IP-Objekte mit unterschiedlichen Bedingungen einrichten.



Objekte >> IP-Objekt

Profile der IP-Objekte: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 >> Weiter >>

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Objekte >> IP-Objekt

Profil: 1

Name:	Technik
Schnittstelle:	beliebig
Addresstyp:	Adressbereich
Start-IP-Adresse:	192.168.1.200
Stopp-IP-Adresse:	192.168.1.240
Subnetz-Maske:	0.0.0.0
Auswahl invertieren:	☐

OK Löschen Abbrechen

Name Geben Sie für dieses Profil eine Bezeichnung ein. Es können bis zu 15 Zeichen eingegeben werden.

Schnittstelle Wählen Sie eine Schnittstelle (WAN, LAN, oder Beliebig).



Die Einstellung **Richtung** unter **Filterregeln ändern** ermöglicht Ihnen beispielsweise die Angabe einer IP-Adresse oder eines IP-Bereichs für das WAN oder LAN oder irgendeine IP-Adresse. Falls Sie hier als **Schnittstelle** LAN angeben und LAN als Richtung unter **Filterregeln ändern** wählen, werden alle mit der LAN-Schnittstelle angegebenen IP-Adressen zur Auswahl auf der Seite **Filterregeln ändern** angeboten.

Adresstyp Bestimmen Sie den Adresstyp der IP-Adresse.

Wählen Sie **Einzelne Adresse**, falls dieses Objekt nur eine einzelne IP-Adresse enthält.
Wählen Sie **Adressbereich**, falls dieses Objekt mehrere IP-Adressen innerhalb eines Bereichs beinhaltet.
Wählen Sie **Subnetz-Adresse**, falls dieses Objekt ein Subnetz für IP-Adressen enthält.
Wählen Sie **Beliebige Adresse**, falls dieses Objekt eine beliebige IP-Adresse enthält.

Start-IP-Adresse Geben Sie eine einzelne IP-Adresse bzw. die Start-IP-Adresse eines Adressbereichs ein.

Stopp-IP-Adresse Geben Sie die Stopp-IP-Adresse des Adressbereichs ein.

Subnetz-Maske Geben Sie die Subnetz-Maske ein, falls als Typ Subnetz-Adresse gewählt wurde.

Auswahl invertieren Falls dieses Kästchen markiert wird, werden alle außer den oben aufgeführten IP-Adressen ausgewählt.

Beispiel für Einstellungen eines IP-Objekts:

Profile der IP-Objekte:

Index	Name
1.	Technik
2.	Verwaltung
3.	RMA
4.	CEO
5.	

4.5.2 IP-Gruppe

Diese Seite ermöglicht Ihnen, mehrere IP-Objekte zu einer IP-Gruppe zu verbinden.

Objekte >> IP-Gruppe

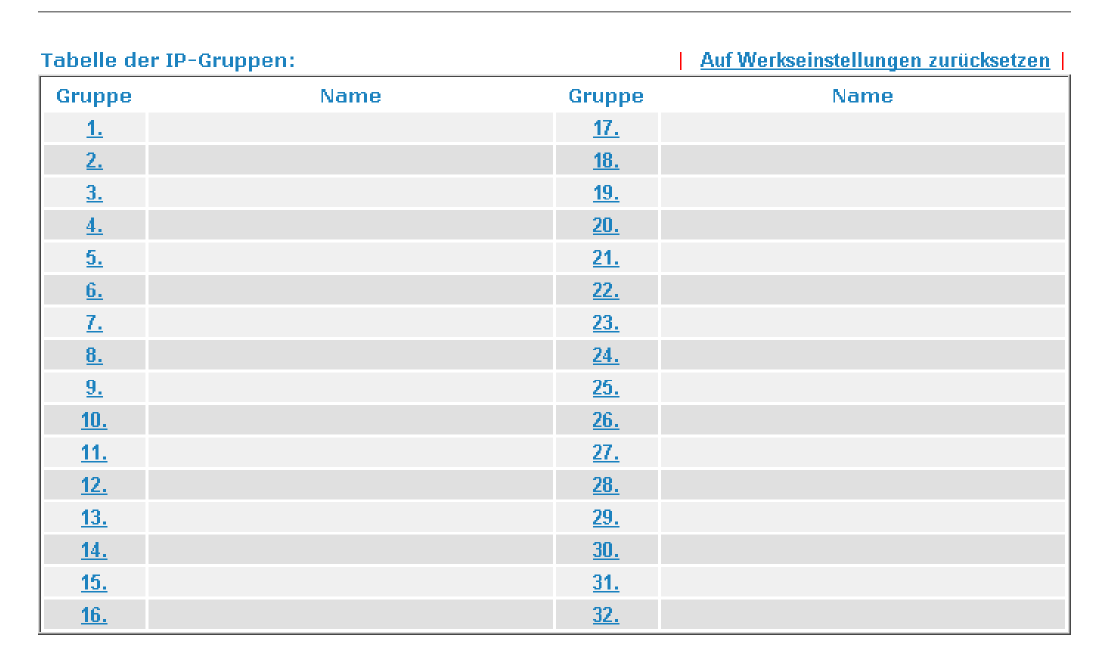


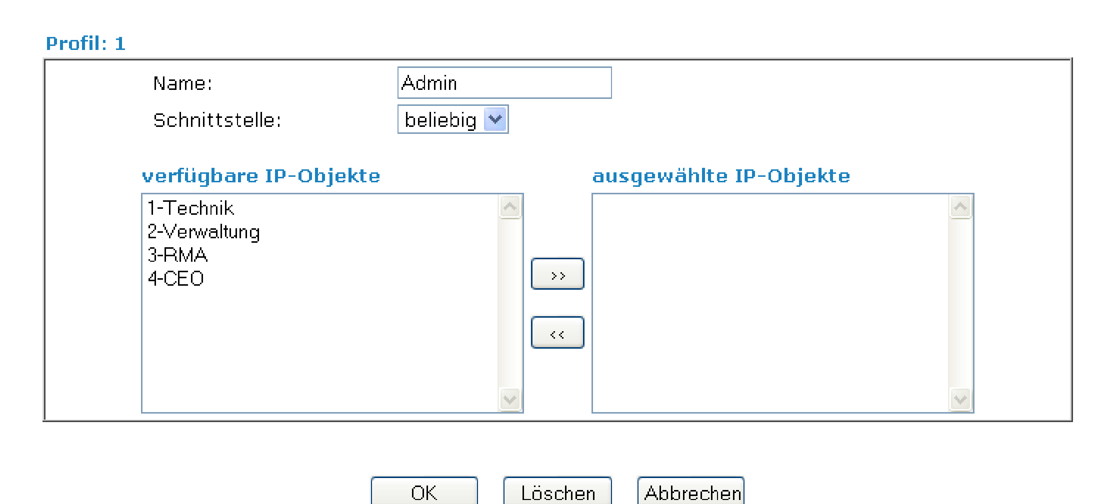
Tabelle der IP-Gruppen: | Auf Werkseinstellungen zurücksetzen |

Gruppe	Name	Gruppe	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Objekte >> IP-Gruppe



Name	Geben Sie für dieses Profil eine Bezeichnung ein. Es können bis zu 15 Zeichen eingegeben werden.
Schnittstelle	Wählen Sie WAN, LAN oder Beliebig, damit alle vorhandenen IP-Objekte mit der angegebenen Schnittstelle angezeigt werden.
Verfügbare IP-Objekte	Sämtliche vorhandene IP-Objekte mit der oben gewählten Schnittstelle werden in diesem Feld angezeigt.
Gewählte IP-Objekte	Klicken Sie auf die Taste >>, um die ausgewählten IP-Objekte in diesem Feld hinzuzufügen.

4.5.3 Servicetyp-Objekt

Sie können bis zu 96 Servicetyp-Objekte mit unterschiedlichen Bedingungen einrichten.

Objekte >> Servicetyp-Objekt

Profile der Servicetyp-Objekte: | Auf Werkseinstellungen zurücksetzen |

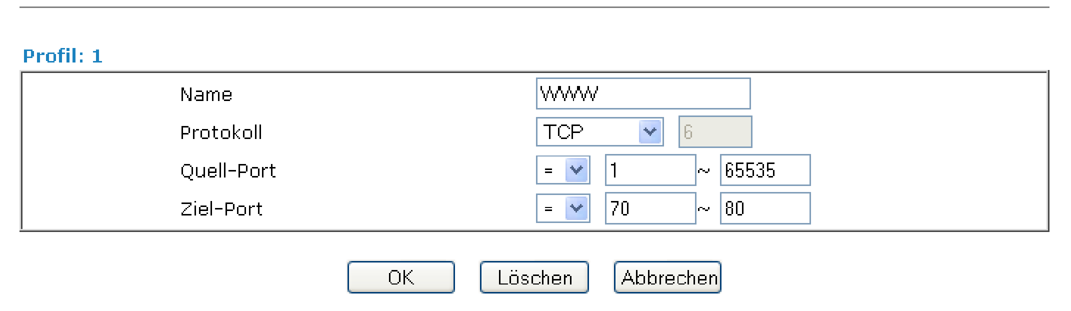
Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 >> Weiter >>

Auf Werkseinstellungen zurücksetzen	Alle Profile löschen.

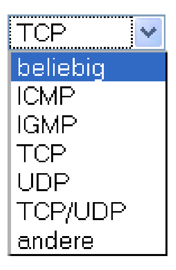
Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Objekte >> Servicetyp-Objekt



Name Geben Sie für dieses Profil eine Bezeichnung ein.

Protokoll Geben Sie das/die Protokoll(e) an, auf welche(s) dieses Profil anzuwenden ist.



Quell-/Ziel-Port Die Spalten **Quellport** und **Zielport** werden für das TCP/UDP-Protokoll benötigt. Bei anderen Protokollen können diese Spalten ignoriert werden. Die Filterregel kann eine beliebige Portnummer ausfiltern.

(=) – Identische erste und letzte Werte weisen auf einen einzelnen Port hin; unterschiedliche erste und letzte Werte weisen auf einen Portbereich hin, der für dieses Profil verfügbar ist.

(!=) – Identische erste und letzte Werte weisen auf alle Ports außer dem hier angegebenen Port hin; unterschiedliche erste und letzte Werte weisen darauf hin, dass alle Ports außer dem hier angegebenen Bereich für diese Servicetyp verfügbar sind.

(>) – Die Portnummer, die größer als dieser Wert ist, ist verfügbar.

(<) – Die Portnummer, die kleiner als dieser Wert ist, ist für dieses Profil verfügbar.

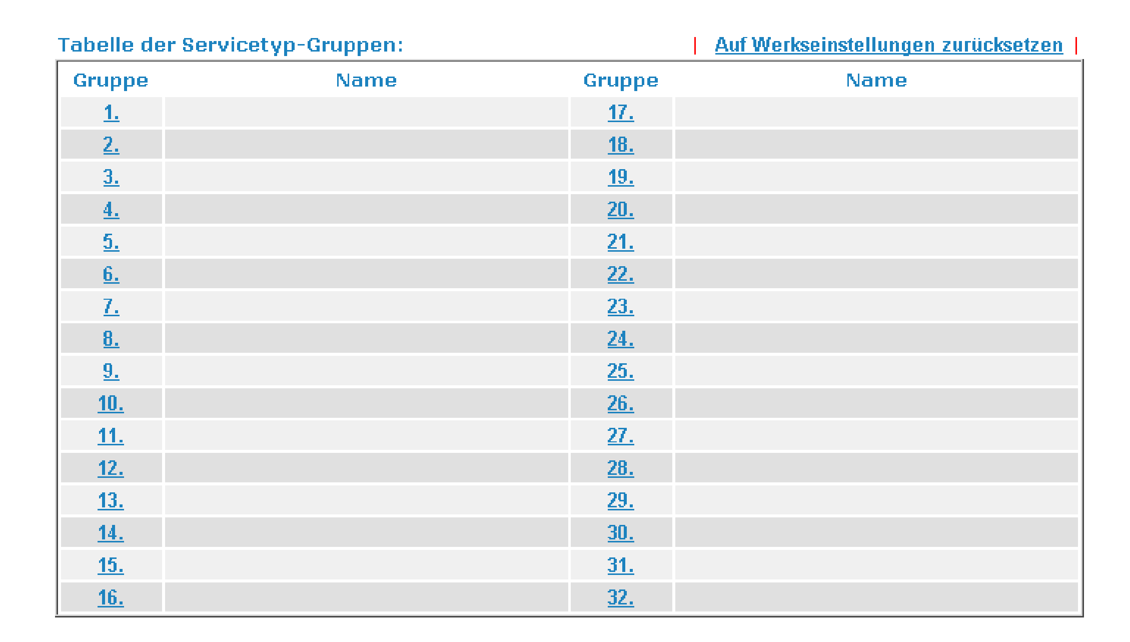
Beispiel für Einstellungen eines Servicetyp-Objekts:

Profile der Servicetyp-Objekte:

Index	Name
1.	WWW
2.	SIP
3.	RTP
4.	

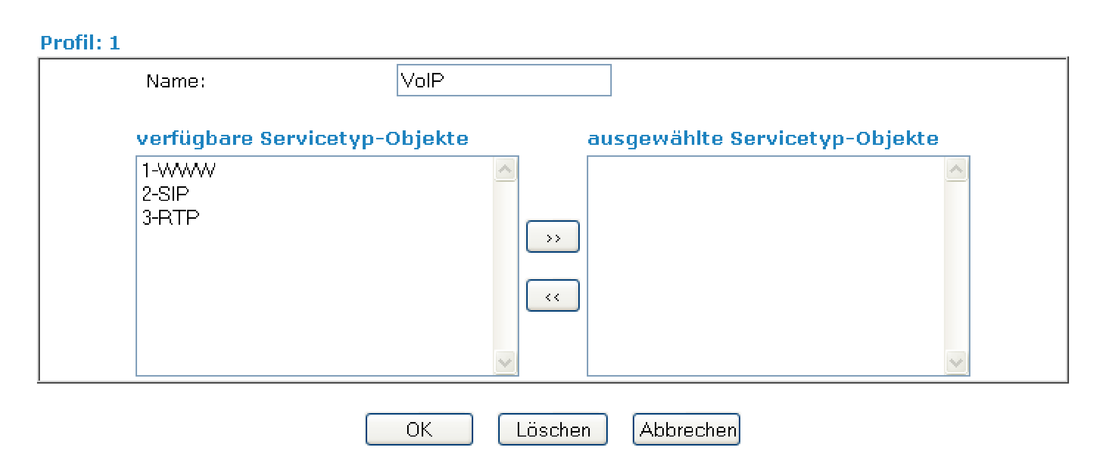
4.5.4 Servicetyp-Gruppe

Diese Seite ermöglicht Ihnen, mehrere Servicetypen zu einer Gruppe zu verbinden.



Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



Bezeichnung	Geben Sie für dieses Profil eine Bezeichnung ein.
Verfügbare Servicetyp-Objekte	Dieses Feld zeigt alle verfügbaren Servicetyp-Objekte an, die Sie unter **Objekte>>Servicetyp-Objekt** hinzugefügt haben.
Ausgewählte Servicetyp-Objekte	Klicken Sie auf die Taste >>, um die ausgewählten IP-Objekte in diesem Feld hinzuzufügen.

4.5.5 Stichwort-Objekt

Sie können bis zu 200 Stichwort-Objektprofile zur Auswahl als Blacklist oder Whitelist unter **CSM >>Inhaltsbezogener URL-Filter/Inhaltsbezogener Web-Filter** einrichten.

Objekte >> Stichwort-Objekt

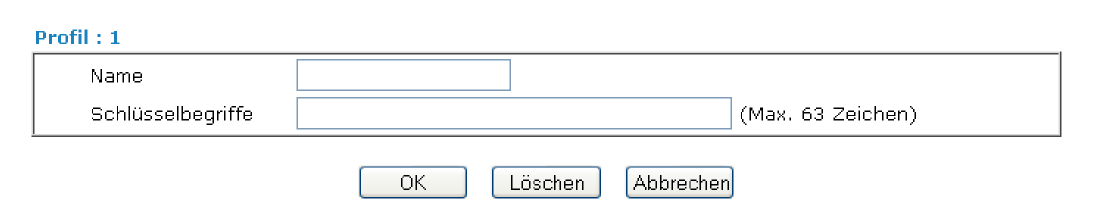
Profile der Stichwort-Objekte: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

<< 1-32 | 33-64 | 65-96 | 97-128 | 129-160 | 161-192 | 193-200 >> Weiter >>

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



Name	Geben Sie für dieses Profil eine Bezeichnung ein, z.B. "Spiel".
Inhalt	Geben Sie den Inhalt des Profils ein, z.B. *Glücksspiel*. Beim Browsen im Internet wird dieser Begriff beobachtet und Seiten, welche diesen Begriff enthalten, gemäß den Firewall-Einstellungen entweder blockiert oder durchgelassen.

4.5.6 Stichwort-Gruppe

Diese Seite ermöglicht Ihnen, mehrere Stichwort-Objekte zu einer Gruppe zu verbinden. Die hier gesetzten Stichwort-Gruppen stehen unter **CSM >>Inhaltsbezogener URL-Filter/Inhaltsbezogener Web-Filter** zur Auswahl als Blacklist oder Whitelist.

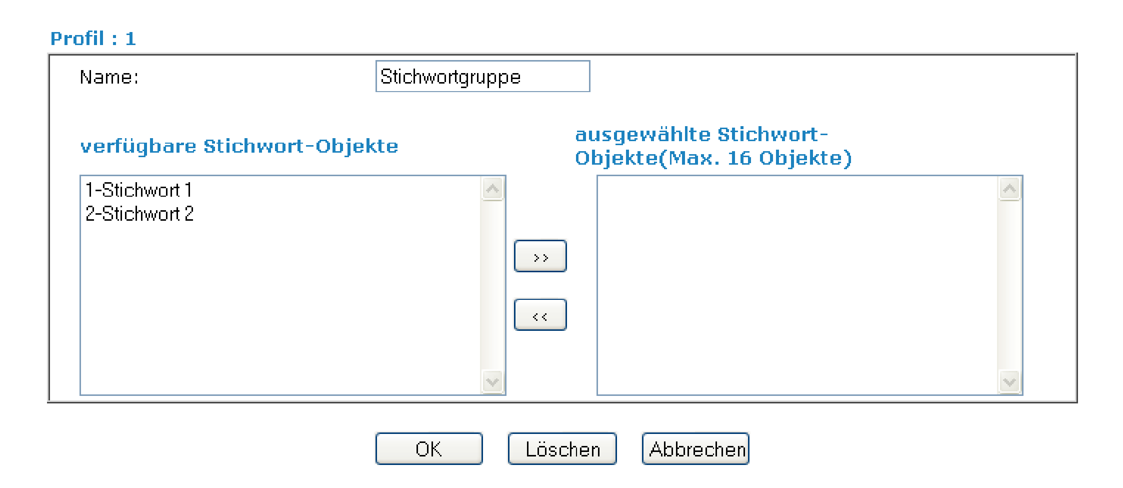
Objekte >> Stichwort-Gruppe

Tabelle der Stichwort-Gruppen: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Index	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.



Name	Geben Sie für diese Gruppe eine Bezeichnung ein.
Verfügbare Stichwort-Objekte	Sie können Stichwort-Objekte von der Seite mit den Stichwort-Objekten zu einer Stichwort-Gruppe zusammenfassen. Sämtliche verfügbare Stichwort-Objekte, die Sie eingerichtet haben, werden in diesem Feld angezeigt.
Ausgewählte Stichwort-Objekte	Klicken Sie auf die Taste », um die ausgewählten Stichwort-Objekte in diesem Feld hinzuzufügen.

4.5.7 Dateiformat-Objekt

Auf dieser Seite können Sie bis zu acht Profile einrichten, die unter **CSM>>Inhaltsbezogener URL-Filter** zur Anwendung kommen. Alle Dateien mit den in diesen Profilen angegebenen Erweiterungen werden gemäß der gewählten Aktion verarbeitet.

Profil 1 mit der Bezeichnung "Standard" ist das Standardprofil. Die Dateien mit den in diesem Profil angegebenen Dateierweiterungen werden ignoriert und vom Vigor-Router nicht gescannt.

Objekte >> Dateiformat-Objekt

Profile der Dateiformat-Objekte: | Auf Werkseinstellungen zurücksetzen |

Profil	Name	Profil	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Auf Werkseinstellungen zurücksetzen	Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte.

Objekte >> Dateiformat-Objekt

Profil: 1 Name:

Kategorien	Dateiformate						
Bilddateien (Alles auswählen / Alles löschen)	.bmp	.dib	.gif	.jpeg	.jpg	.jpg2	.jp2
	.pct	.pcx	.pic	.pict	.png	.tif	.tiff
Video-Dateien (Alles auswählen / Alles löschen)	.asf	.avi	.mov	.mpe	.mpeg	.mpg	.mp4
	.qt	.rm	.wmv	.3gp	.3gpp	.3gpp2	.3g2
Audio-Dateien (Alles auswählen / Alles löschen)	.aac	.aiff	.au	.mp3	.m4a	.m4p	.ogg
	.ra	.ram	.vox	.wav	.wma		
Java (Alles auswählen / Alles löschen)	.class	.jad	.jar	.jav	.java	.jcm	.js
	.jse	.jsp	.jtk				
ActiveX (Alles auswählen / Alles löschen)	.alx	.apb	.axs	.ocx	.olb	.ole	.tlb
	.viv	.vrm					
Kompressionen (Alles auswählen / Alles löschen)	.ace	.arj	.bzip2	.bz2	.cab	.gz	.gzip
	.rar	.sit	.zip				
Ausführbare Dateien (Alles auswählen / Alles löschen)	.bas	.bat	.com	.exe	.inf	.pif	.reg
	.scr						

OK Löschen Abrechen

Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie alle Dateierweiterungen, die von dem Router bearbeitet werden sollen. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

4.5.8 IM-Objekt

Auf dieser Seite können Sie bis zu 32 Profile für Instant Messenger einrichten. Diese Profile kommen unter **CSM>>IM-/P2P-Filter** als Filter zur Anwendung.

Objekte >> IM-Objekt

Profile der IM-Objekte: | Auf Werkseinstellungen zurücksetzen |

Profil	Name	Profil	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte. Es werden verschiedene Instant Messenger (IM) aufgeführt, deren Benutzung Sie sperren können. Markieren Sie einfach die entsprechenden Kästchen und klicken auf **OK**. Auf der Seite **CSM>>IM-/P2P-Filter** können Sie die Dropdown-Liste **IM-Objekt** verwenden, um das richtige Profil als Standard für die folgenden Hosts zu wählen.

Objekte >> IM-Objekt

Profil-Index: 1

Profilname:

Auswahl wird blockiert:

weitere IM-Anwendungen				VoIP
☐ MSN	☐ YahooIM	☐ AIM	☐ ICQ	☐ Skype
☐ QQ	☐ iChat	☐ Jabber/GoogleTalk	☐ GoogleChat	☐ SIP

Web IM (* = mehrere Web-Adressen)					
☐ Web-IM-URLs	eMessenger	WebMSN	meebo*	eBuddy	ILoveIM*
	ICQ Java*	ICQ Flash*	goowy*	IMhaha*	getMessenger
	IMUnitive*	Wablet*	mabber*	MSN2GO*	KoolIM
	MessengerFX*	MessengerAdictos	WebYahooIM		

OK Löschen Abbrechen

Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie sämtliche Punkte, die der Host nicht benutzen darf. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

4.5.9 P2P-Objekt

Auf dieser Seite können Sie bis zu 32 Profile für P2P-Anwendungen einrichten. Diese Profile kommen unter **CSM>>IM-/P2P-Filter** als Filter zur Anwendung.

Objekte >> P2P-Objekt

Profile der P2P-Objekte: | Auf Werkseinstellungen zurücksetzen |

Profil	Name	Profil	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte. Es werden verschiedene P2P-Protokolle aufgeführt, deren Benutzung Sie sperren können. Markieren Sie einfach die entsprechenden Kästchen und klicken auf **OK**. Auf der Seite **CSM>>IM-/P2P-Filter** können Sie später die Dropdown-Liste **P2P-Objekt** verwenden, um das richtige Profil als Standard für die folgenden Hosts zu wählen.

Objekte >> P2P Object Profile

Profil-Index: 1

Profilname:

Auswahl wird blockiert:

Protokoll	Anwendungen
☐ SoulSeek	SoulSeek
☐ eDonkey	eDonkey, eMule, Shareaza
☐ FastTrack	KazaA, BearShare, iMesh
☐ OpenFT	KCeasy, FilePipe
☐ Gnutella	BearShare, Limewire, Shareaza, Foxy
☐ OpenNap	Lopster, XNap, WinLop
☐ BitTorrent	BitTorrent, BitSpirit, BitComet
☐ Winny	Winny, WinMX, Share

OK Löschen Abbrechen

Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie sämtliche Protokolle, die der Host nicht benutzen darf. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

4.5.10 Diverses

Auf dieser Seite können Sie bis zu 32 Profile für verschiedene Anwendungen einrichten. Diese Profile kommen unter **CSM>>IM-/P2P-Filter** als Filter zur Anwendung.

Objekte >> Diverses

Profile der diversen Objekte: | Auf Werkseinstellungen zurücksetzen |

Profil	Name	Profil	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie für die Detailkonfiguration auf eine Nummer in der Profilspalte. Auf der Seite werden Tunnel- und Streaming-Anwendungen aufgeführt, deren Benutzung Sie sperren können. Markieren Sie einfach die entsprechenden Kästchen und klicken auf **OK**. Auf der Seite **CSM>>IM-/P2P-Filter** können Sie später die Dropdown-Liste **Diverse Objekte** verwenden, um das entsprechende Profil als Standard für die folgenden Hosts zu wählen.

Objekte >> MDiverses

Profil-Index: 1

Profilname:

Auswahl wird blockiert:

Streaming			
☐ MMS	☐ RTSP	☐ TVAnts	☐ PPStream
☐ PPlive	☐ FeiDian	☐ UUSee	☐ NSPlayer
☐ PCAST	☐ TVKoo	☐ SopCast	☐ UDLiveX
☐ TVUPlayer	☐ MySee	☐ Joost	☐ FlashVideo

OK | Löschen | Abbrechen

Profilname Geben Sie für dieses Profil einen Namen ein.

Geben Sie für das Profil eine Bezeichnung ein und markieren Sie sämtliche Protokolle, die der Host nicht benutzen darf. Klicken Sie abschließend auf **OK**, um das Profil zu speichern.

4.6 CSM-Profil

Content Security Management (CSM)

CSM ist die Abkürzung für **Content Security Management**, einer Funktion zur Steuerung der IM/P2P-Nutzung und Filterung von Web- und URL-Inhalten.

Die Verbreitung verschiedener Instant Messenger Anwendungen hat die Kommunikation enorm vereinfacht. Während einige Unternehmen diese als nützliche Tools für Kundenkontakte fördern, befürchten andere Unternehmen jedoch den Missbrauch solcher Anwendungen während der Arbeitszeit oder unbekannte Sicherheitsrisiken. Die Situation ist bei P2P-Anwendungen ähnlich, da File Sharing zwar praktisch, aber auch unsicher sein kann. Die CSM-Funktionalität des Routers trägt diesen Anforderungen Rechnung.

IM/P2P-Filter

Die Verbreitung verschiedener Instant Messenger Anwendungen hat die Kommunikation enorm vereinfacht. Während einige Unternehmen diese als nützliche Tools für Kundenkontakte fördern, befürchten andere Unternehmen jedoch den Missbrauch solcher Anwendungen während der Arbeitszeit oder unbekannte Sicherheitsrisiken. Die Situation ist bei P2P-Anwendungen ähnlich, da File Sharing zwar praktisch, aber auch unsicher sein kann. Die CSM-Funktionalität des Routers trägt diesen Anforderungen Rechnung.

Inhaltsbezogener URL-Filter

Um Benutzern eine geeignete Arbeitsumgebung zu schaffen, verfügt der Vigor-Router über einen **inhaltsbezogenen URL-Filter**, mit dem der unerwünschte Zugang von/zu unpassenden Web-Seiten vermieden wird und Web-Inhalte gesperrt werden, in denen sich bösartiger Code verbergen könnte.

Wenn ein Benutzer eine URL anklickt oder eingibt, die unerwünschte Stichwörter enthält, wird der HTTP-Request für die jeweilige Web-Seite durch den URL-Stichwortfilter blockiert, so dass der Benutzer keinen Zugriff auf die Seite hat. Man könnte sich den **inhaltsbezogenen URL-Filter** als gewissenhaften Verkäufer vorstellen, der Teenagern keine Zeitschriften verkauft, die nicht jugendfrei sind. Im Büro sorgt der **inhaltsbezogene URL-Filter** dafür, dass nur auf betrieblich relevante Inhalte zugegriffen werden kann, um die Arbeitsleistung zu steigern. Ein inhaltsbezogener URL-Filter ist in Bezug auf die Filterung wirkungsvoller als eine konventionelle Firewall. Dies liegt daran, dass der Filter die URL-Zeichenfolgen und einige der HTTP-Daten, die sich im Nutzdatenteil der TCP-Pakete verbergen, überprüft, während traditionelle Firewalls Pakete lediglich anhand der Felder in TCP/IP-Headern überprüfen.

Außerdem kann der Vigor-Router Benutzer davon abhalten, aus Versehen schädlichen Code von Web-Seiten herunterzuladen. Schädlicher Code verbirgt sich oft in ausführbaren Objekten wie ActiveX, Java Applets, komprimierten Dateien und anderen ausführbaren Dateien. Das Herunterladen solcher Dateien von Web-Seiten kann eine Bedrohung für Ihr System darstellen. Ein ActiveX-Control-Objekt wird oft verwendet, um eine interaktive Web-Funktion zu ermöglichen. Schädlicher Code, der sich in diesem Objekt verbirgt, kann so auf das System des Benutzers gelangen.

Inhaltsbezogener Web-Filter

Wir alle sind uns bewusst, dass Internetinhalte bisweilen unangebracht sein können, wie dies auch bei anderen Medien der Fall sein kann. Als verantwortlicher Elternteil oder Arbeitgeber sollten Sie die Personen, die Ihnen anvertraut sind, vor Gefahren schützen. Mit dem Web-Filterdienst des Vigor-Routers können Sie Ihr Unternehmen vor üblichen

direkten Gefahren schützen, welche Produktivität, gesetzliche Haftung, Netzwerk und Sicherheit bedrohen. Eltern können ihre Kinder vor dem Laden nicht jugendfreier Web-Seiten oder Chaträumen schützen.

Wenn Sie die Web-Filterfunktion des Vigor-Routers aktivieren und die Kategorien einrichten, die Sie einschränken möchten, wird jede angeforderte URL (z.B. www.bbc.co.uk) mit unserer Server-Datenbank abgeglichen. Diese Datenbank wird regelmäßig aktualisiert (dazu zählen natürlich auch lokale Angebote). Der Server fragt die URL ab und liefert Ihrem Router eine Kategorie. Ihr Vigor-Router entscheidet dann anhand der von Ihnen gewählten Kategorien, ob der Zugriff auf diese Seite erlaubt wird oder nicht. Da die Last auf verschiedene Datenbankserver verteilt wird, die Millionen von Kategorisierungsanfragen beantworten können, besteht kein Grund, durch diese Aktion eine Verzögerung beim Surfen zu befürchten.

Hinweis: Der inhaltsbezogene URL-Filter hat eine höhere Priorität als der inhaltsbezogene Web-Filter.

CSM
- IM-/P2P-Filter
- Inhaltsbezogener URL-Filter
- Inhaltsbezogener Web-Filter

4.6.1 IM-/P2P-Filter

Sie können für verschiedene IM (Instant Messenger)/P2P (Peer to Peer) Anwendungen unterschiedliche Profile einrichten. Die CSM-Profile können im Filtereinrichtungsmenü benutzt werden.

CSM >> IM-/P2P-Filter

Profile für IM/P2P-Anwendungen:: | Auf Werkseinstellungen zurücksetzen |

Profil	Name	Profil	Name
1.		17.	
2.		18.	
3.		19.	
4.		20.	
5.		21.	
6.		22.	
7.		23.	
8.		24.	
9.		25.	
10.		26.	
11.		27.	
12.		28.	
13.		29.	
14.		30.	
15.		31.	
16.		32.	

Auf Werkseinstellungen zurücksetzen Alle Profile löschen.

Klicken Sie auf die Nummer in der Indexspalte, um zu den Detaileinstellungen zu gelangen.

Bezeichnung Geben Sie einen Namen für das CSM-Profil ein.

CSM >> IM/P2P Filter Profile

Profil Index: 1
Bezeichnung:

IM-Objekt	Auswahl
P2P-Objekt	Auswahl
Diverses	Auswahl

OK Abbrechen

Jedes Profil kann bis zu drei Objekteinstellungen enthalten: IM-Objekt, P2P-Objekt und diverses Objekt. Ein solches Profil kann unter **Firewall>>Basiskonfiguration** und **Firewall>>Filtereinstellung** als Standard für die folgenden Hosts bestimmt werden.

4.6.2 Inhaltsbezogener URL-Filter

Um Benutzern eine geeignete Arbeitsumgebung zu schaffen, verfügt der Vigor-Router über einen **inhaltsbezogenen URL-Filter**, mit dem der unerwünschte Zugang von/zu unpassenden Web-Seiten vermieden wird und Web-Inhalte gesperrt werden, in denen sich bösartiger Code verbergen könnte.

Wenn ein Benutzer eine URL anklickt oder eingibt, die unerwünschte Stichwörter enthält, wird der HTTP-Request für die jeweilige Web-Seite durch den URL-Stichwortfilter blockiert, so dass der Benutzer keinen Zugriff auf die Seite hat. Man könnte sich den **inhaltsbezogenen URL-Filter** als gewissenhaften Verkäufer vorstellen, der Teenagern keine Zeitschriften verkauft, die nicht jugendfrei sind. Im Büro sorgt der **inhaltsbezogene URL-Filter** dafür, dass nur auf betrieblich relevante Inhalte zugegriffen werden kann, um die Arbeitsleistung zu steigern. Ein inhaltsbezogener URL-Filter ist in Bezug auf die Filterung wirkungsvoller als eine konventionelle Firewall. Dies liegt daran, dass der Filter die URL-Zeichenfolgen und einige der HTTP-Daten, die sich im Nutzdatenteil der TCP-Pakete verbergen, überprüft, während traditionelle Firewalls Pakete lediglich anhand der Felder in TCP/IP-Headern überprüfen.

Außerdem kann der Vigor-Router Benutzer davon abhalten, aus Versehen schädlichen Code von Web-Seiten herunterzuladen. Schädlicher Code verbirgt sich oft in ausführbaren Objekten wie ActiveX, Java Applets, komprimierten Dateien und anderen ausführbaren Dateien. Das Herunterladen solcher Dateien von Web-Seiten kann eine Bedrohung für Ihr System darstellen. Ein ActiveX-Control-Objekt wird oft verwendet, um eine interaktive Web-Funktion zu ermöglichen. Schädlicher Code, der sich in diesem Objekt verbirgt, kann so auf das System des Benutzers gelangen.

Falls Sie beispielsweise Wörter wie "Sex" hinzufügen, blockiert der Vigor-Router den Zugriff auf Web-Sites oder Web-Seiten wie "www.sex.com" oder www.backdoor.net/images/sex/p_386.html. Sie können auch einfach die gesamte URL (z.B. "www.sex.com") oder einen Teil davon (z.B. "sex.com") angeben.

Der Vigor-Router wird jegliche Anforderungen verwerfen, die versuchen, schädlichen Code abzurufen.

Klicken Sie auf **CSM** und wählen Sie **Inhaltsbezogener URL-Filter**, um die Konfigurationsseite für das Profil zu öffnen.

CSM >> Inhaltsbezogener URL-Filter

Tabelle der inhaltsbezogenen URL-Filter: | Auf Werkseinstellungen zurücksetzen |

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Benutzerhinweis beim Blockieren von Web-Inhalten (max. 255 Zeichen)

```
<body><center><br><p>The requested Web page has been blocked by URL Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

OK

Sie können bis zu acht Profile als inhaltsbezogene URL-Filter setzen. Klicken Sie einfach die Indexnummer unter Profil an, um die folgende Web-Seite zu öffnen.

CSM >> Inhaltsbezogener URL-Filter

Profil-Index: 1

Name:

Priorität: beides durchlassen Log: aus

1. URL-Zugriffskontrolle

aktiv Seitenaufrufe durch Eingabe der IP-Adresse unterbinden

Aktion: durchlassen Auswahl von Gruppen und Objekten Ändern

2. Web-Features

aktiv

Aktion: durchlassen Cookies Proxy Dateiformat-Profil: aus

OK Löschen Abbrechen

Profilname Geben Sie den Profilnamen ein.

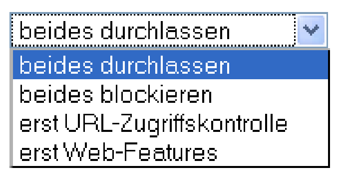
Priorität Bestimmt die Aktion, die der Router durchführen wird.

Beides durchlassen – Der Router lässt alle Pakete durch, die den unter URL-Zugriffskontrolle und Web-Features unten angegebenen Bedingungen entsprechen. Falls Sie diese Einstellung wählen, werden die Konfigurationen für die URL-Zugriffskontrolle und Web-Features auf dieser Seite deaktiviert.

Beides blockieren –Der Router blockiert alle Pakete, die den unter URL-Zugriffskontrolle und Web-Features unten angegebenen Bedingungen entsprechen. Falls Sie diese Einstellung wählen, werden die Konfigurationen für die URL-Zugriffskontrolle und Web-Features auf dieser Seite deaktiviert.

Erst URL-Zugriffskontrolle – Falls alle Pakete den Bedingungen entsprechen, die unter URL-Zugriffskontrolle und Web-Features unten angegeben sind, kann dies die Priorität der ausgeführten Aktion bestimmen. Bei dieser Option verarbeitet der Router die Pakete zunächst mit den Bedingungen für URLs und dann mit den Bedingungen für Web-Features wie unten angegeben.

Erst Web-Features – Falls alle Pakete den Bedingungen entsprechen, die unter URL-Zugriffskontrolle und Web-Features unten angegeben sind, kann dies die Priorität der ausgeführten Aktion bestimmen. Bei dieser Option verarbeitet der Router die Pakete zunächst mit den Bedingungen für Web-Features und dann mit den Bedingungen für URLs wie unten angegeben.



Log

Keine – Für dieses Profil wird keine Log-Datei aufgezeichnet.

Durchlassen – Lediglich Meldungen zum Durchlassen werden im Syslog aufgezeichnet.

Blockieren – Lediglich Meldungen zum Blockieren werden im Syslog aufgezeichnet.

Alle – Alle Aktionen (Durchlassen und Blockieren) werden im Syslog aufgezeichnet.



URL-Zugriffskontrolle

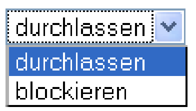
Aktiv - Markieren Sie dieses Kästchen, um die URL-Zugriffskontrolle zu aktivieren. Beachten Sie, dass die Priorität der **URL-Zugriffskontrolle** höher ist als die der **Web-Features**. Falls der Web-Inhalt den Einstellungen der URL-Zugriffskontrolle entspricht, führt der Router die in diesem Feld angegebene Aktion aus und ignoriert die unter Web-Features angegebene Aktion.

Seitenaufrufe durch Eingabe der IP-Adresse unterbinden - Markieren Sie dieses Kästchen, um Surfen durch Eingabe der IP-Adresse (z.B. http://202.6.3.2) zu unterbinden. Dadurch kann vermieden werden, dass jemand die URL-Zugriffskontrolle umgeht. Sie müssen Ihren Browser-Cache zunächst löschen, damit die inhaltsbezogene URL-Filterfunktion auf zuvor besuchten Web-Seiten ordnungsgemäß funktioniert.

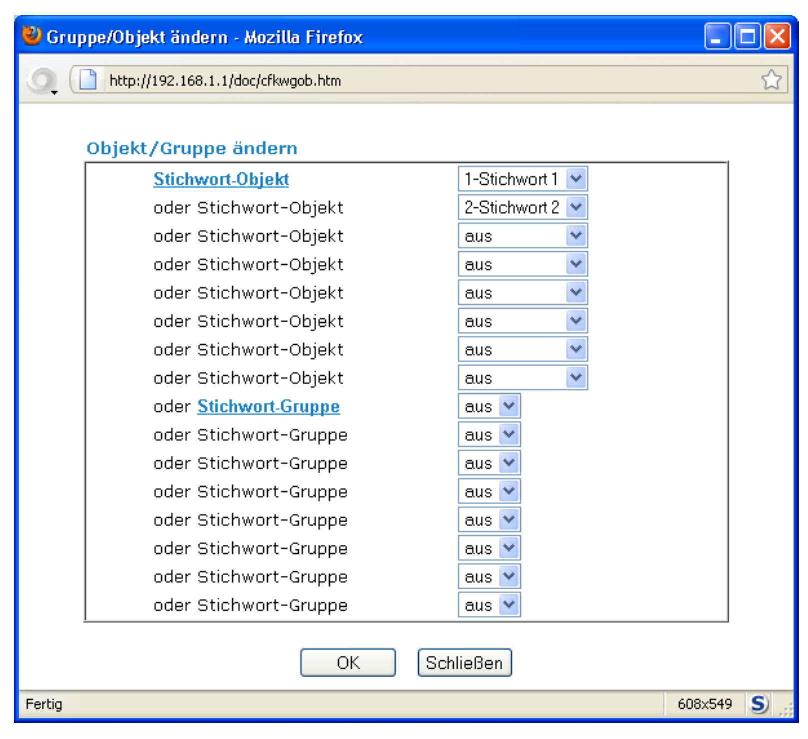
Aktion – Diese Einstellung ist nur verfügbar, falls entweder **Erst URL-Zugriffskontrolle** oder **Erst Web-Features** gewählt wurde. ***Durchlassen*** - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern zulassen.

Blockieren - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern blockieren.

Falls die Web-Seiten nicht den hier angegebenen Stichwörtern entsprechen, werden sie mit der entgegengesetzten Aktion verarbeitet.



Auswahl von Gruppen und Objekten – Der Vigor-Router ermöglicht Benutzern die Definition von Stichwörtern, wobei jedes Frame die Angabe von mehreren Stichwörtern erlaubt. Das Stichwort kann ein Nomen, ein Teil davon oder eine komplette URL sein. Mehrere Stichwörter innerhalb eines Frames werden durch Leerzeichen, Komma oder Semikolon getrennt. Die maximale Länge jedes Frames beträgt 32 Zeichen. Nach Angabe von Stichwörtern wird der Vigor-Router Verbindungen zur Web-Site ablehnen, deren URL-Zeichenfolge irgendeinem benutzerdefinierten Stichwort entspricht. Je einfacher die Liste der zu blockierenden Stichwörter ist, desto effizienter wird der Vigor-Router arbeiten.



Web-Features

Aktiv - Markieren Sie dieses Kästchen, damit das Stichwort blockiert bzw. durchgelassen wird.

Aktion – Diese Einstellung ist nur verfügbar, falls entweder **Erst URL-Zugriffskontrolle** oder **Erst Web-Features** gewählt wurde. **Durchlassen** erlaubt den Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern.

***Durchlassen* -** Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern zulassen.

***Blockieren* -** Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Stichwörtern blockieren.

Falls die Web-Seiten nicht den hier angegebenen Features entsprechen, werden sie mit der entgegengesetzten Aktion verarbeitet.

Cookies - Markieren Sie dieses Kästchen, um die Übertragung von Cookies zu unterbinden, um die Privatsphäre des lokalen Benutzers zu schützen.

Proxy - Markieren Sie dieses Kästchen, um jegliche Proxy-Übertragung abzulehnen.

Dateiformat-Profil – Wählen Sie eines der Profile, das Sie bereits unter **Objekte>> Dateiformat-Objekt** zum Durchlassen oder Blockieren von Datei-Downloads eingerichtet haben.



4.6.3 Inhaltsbezogener Web-Filter

Wir alle sind uns bewusst, dass Internetinhalte bisweilen unangebracht sein können, wie dies auch bei anderen Medien der Fall sein kann. Als verantwortlicher Elternteil oder Arbeitgeber sollten Sie die Personen, die Ihnen anvertraut sind, vor Gefahren schützen. Mit dem Web-Filterdienst des Vigor-Routers können Sie Ihr Unternehmen vor üblichen direkten Gefahren schützen, welche Produktivität, gesetzliche Haftung, Netzwerk und Sicherheit bedrohen. Eltern können ihre Kinder vor dem Laden nicht jugendfreier Web-Seiten oder Chaträumen schützen.

Wenn Sie die Web-Filterfunktion des Vigor-Routers aktivieren und die Kategorien einrichten, die Sie einschränken möchten, wird jede angeforderte URL (z.B. www.bbc.co.uk) mit unserer Server-Datenbank abgeglichen. Diese Datenbank wird regelmäßig aktualisiert (dazu zählen natürlich auch lokale Angebote). Der Server fragt die URL ab und liefert Ihrem Router eine Kategorie. Ihr Vigor-Router entscheidet dann anhand der von Ihnen gewählten Kategorien, ob der Zugriff auf diese Seite erlaubt wird oder nicht. Da die Last auf verschiedene Datenbankserver verteilt wird, die Millionen von Kategorisierungsanfragen beantworten können, besteht kein Grund, durch diese Aktion eine Verzögerung beim Surfen zu befürchten.

Klicken Sie auf **CSM** und wählen Sie **Inhaltsbezogener Web-Filter**, um die Konfigurationsseite für das Profil zu öffnen.

CSM >> Inhaltsbezogener Web-Filter

Tabelle der inhaltsbezogenen Web-Filter: | Auf Werkseinstellungen zurücksetzen |

Profile	Name	Profile	Name
1.		5.	
2.		6.	
3.		7.	
4.		8.	

Inhaltsbezogener Web-Filter

Server auswählen: globale Webseiten
Webseite testen und kategorisieren lassen

Benutzerhinweis beim Blockieren von Web-Inhalten (max. 255 Zeichen)

```
<body><center><br><p>The requested Web page has been blocked by Web Content Filter.
<p>Please contact your system administrator for further information.</center></body>
```

OK

Sie können bis zu acht Profile als inhaltsbezogene Web-Filter setzen. Klicken Sie einfach die Indexnummer unter Profil an, um die folgende Web-Seite zu öffnen.

CSM >> Inhaltsbezogener Web-Filter

Profil-Index : 1

Name:

Action : blockieren **Log :** blockieren

Gruppen	Kategorien		
Kinderschutz Alles auswählen Alles löschen	Chat Geldspiele Pornografie	Kriminalität Hacken/Cracken Gewalt	Drogen/Alkohol Hassreden Waffen
Freizeit Alles auswählen Alles löschen	Werbung Spiele Hobby Persönliches Sport	Unterhaltung Glanz und Glamour Lifestyle Fotosuche Streaming Medien	Essen Gesundheit Fahrzeuge Einkaufen Reisen
Geschäftliches Alles auswählen Alles löschen	Computer/Internet Politik Remote Proxys	Finanzen Vermögen Suchmachinen	Job Suche/Karriere Referenz Web-Mail
Andere Alles auswählen Alles löschen	Bildung News Usenet News	Hosting Seiten Religion nicht-kategorisierte Webseiten	Kinderseiten Sexualerziehung

OK Löschen Abbrechen

Aktion

Durchlassen - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Kategorien zulassen.

Blockieren - Zugriff auf die entsprechende Web-Seite mit den im Feld unten aufgeführten Kategorien blockieren.

Falls die Web-Seiten nicht den hier angegebenen Features entsprechen, werden sie mit der entgegengesetzten Aktion verarbeitet.

Log

Keine – Für dieses Profil wird keine Log-Datei aufgezeichnet.

Durchlassen – Lediglich Meldungen zum Durchlassen werden im Syslog aufgezeichnet.

Blockieren – Lediglich Meldungen zum Blockieren werden im Syslog aufgezeichnet.

Alle – Alle Aktionen (Durchlassen und Blockieren) werden im Syslog aufgezeichnet.



Sehen Sie hierzu auch die Benutzerinformation zum **Inhaltsbezogenen Web-Filter**.

4.7 Bandbreitenmanagement

Die folgende Abbildung zeigt die Menüeinträge für das Bandbreitenmanagement:

Bandwidth Management
- Sessions Limit
- Bandwidth Limit
- Quality of Service

4.7.1 Sitzungen begrenzen

Ein PC mit einer privaten IP-Adresse kann über den NAT-Router auf das Internet zugreifen. Der Router erzeugt für eine solche Verbindung die Einträge der NAT-Sitzung. P2P (Peer to Peer) Anwendungen (z.B. BitTorrent) benötigen immer viele Sitzungen für den Betrieb und belegen oft so viele Ressourcen, dass wichtige Zugriffe behindert werden. Um dieses Problem zu lösen, können Sie die Anzahl der Sitzungen für die angegebenen Hosts beschränken.

Klicken Sie im Menü **Bandbreitenmanagement** auf **Sitzungen begrenzen**, um die entsprechende Web-Seite zu öffnen.

Bandwidth Management >> Sessions Limit

Sessions Limit

Enable Disable

Default Max Sessions: 100

Limitation List

Index Start IP End IP Max Sessions

Specific Limitation

Start IP: End IP:

Maximum Sessions:

Add Edit Delete

Time Schedule

Index(1-15) in Schedule Setup: , , ,

Note: Action and Idle Timeout settings will be ignored.

OK

Um die Funktion zur Begrenzung von Sitzungen zu aktivieren, klicken Sie einfach auf **Aktiv** und geben die Standardgrenze für Sitzungen ein.

Aktiv	Klicken Sie auf diese Taste, um die Sitzungsbegrenzungsfunktion zu aktivieren.
Inaktiv	Klicken Sie auf diese Taste, um die Sitzungsbegrenzungsfunktion zu deaktivieren.
Standard Sitzungslimit	Legt die standardmäßige Anzahl der Sitzungen für jeden Rechner im LAN fest.
Begrenzungsliste	Zeigt eine Liste spezifischer Begrenzungen an, die Sie auf dieser Web-Seite eingerichtet haben.
Start-IP	Bestimmt die Start-IP-Adresse für die Sitzungsbegrenzung
End-IP	Bestimmt die End-IP-Adresse für die Sitzungsbegrenzung.
Maximale Sitzungen	Gibt die verfügbare Anzahl der Sitzungen für jeden Host im angegebenen IP-Adressbereich an. Falls Sie in diesem Feld keine Anzahl von Sitzungen angeben, verwendet das System das Standard-Sitzungslimit für die von Ihnen für jeden Index gesetzte spezifische Begrenzung.
Hinzufügen	Fügt der obigen Liste die spezifische Sitzungsbegrenzung hinzu.
Bearbeiten	Ermöglicht Ihnen, die Einstellungen der gewählten Begrenzung zu bearbeiten.
Entfernen	Gewählte Einstellungen von der Begrenzungsliste entfernen.
Index (1-15) in der Timerkonfiguration	Sie können für Ihre Anforderungen vier Timer einrichten. Alle Timer können im Voraus auf der Web-Seite **Anwendungen – Timer** eingestellt werden, und Sie können die Nummer verwenden, die Sie auf jener Web-Seite gesetzt haben.

4.7.2 Bandbreitenbegrenzung

Der Downstream- und Upstream-Datenfluss von FTP-, HTTP- und einigen P2P-Anwendungen kann viel Bandbreite in Anspruch nehmen und somit andere Anwendungen beeinträchtigen. Sie können die Bandbreitenbegrenzung einsetzen, um die Bandbreite effizienter zu nutzen.

Klicken Sie im Menü **Bandbreitenmanagement** auf **Bandbreite begrenzen**, um die entsprechende Web-Seite zu öffnen.

Bandbreitenmanagement >> Bandbreite begrenzen

Bandbreite begrenzen

aktiv   Anwenden auf Routing-Subnetz   inaktiv

Standard TX-Begrenzung: 200 kbit/s

Standard RX-Begrenzung: 800 kbit/s

Begrenzungsliste

Index Start-IP End-IP max. TX max. RX

spezielle Begrenzung

Start-IP: End-IP:

max. TX: kbit/s max. RX: kbit/s

Hinzufügen Bearbeiten Löschen

Verbindungstimer

Index (1-15) aus der Verbindungstimer Konfiguration: , , ,

Hinweis: Einstellungen in "Aktion" und "Leerlaufzeit" werden ignoriert.

OK

Um die Funktion zur Bandbreitenbegrenzung zu aktivieren, klicken Sie einfach auf **Aktiv** und geben die Standardgrenzen für Upstream und Downstream ein.

Aktiv	Klicken Sie auf diese Taste, um die Bandbreitenbegrenzungsfunktion zu aktivieren.
Inaktiv	Klicken Sie auf diese Taste, um die Bandbreitenbegrenzungsfunktion zu deaktivieren.
Standard TX-Begrenzung	Definieren Sie die Standard-Upstream-Geschwindigkeit für jeden Rechner im LAN.
Standard RX-Begrenzung	Definieren Sie die Standard-Downstream-Geschwindigkeit für jeden Rechner im LAN.
Begrenzungsliste	Zeigt eine Liste spezifischer Begrenzungen an, die Sie auf dieser Web-Seite eingerichtet haben.
Start-IP	Geben Sie die Start-IP für die Begrenzung der Bandbreite ein.
End-IP	Geben Sie die End-IP für die Begrenzung der Bandbreite ein.
Max. TX	Bestimmen Sie die Begrenzung für die Upstream-Geschwindigkeit. Falls Sie in diesem Feld keine Grenze angeben, verwendet das System die Standardgeschwindigkeit für die von Ihnen für jeden Index gesetzte spezifische Begrenzung.

Max. RX	Bestimmen Sie die Begrenzung für die Downstream-Geschwindigkeit. Falls Sie in diesem Feld keine Grenze angeben, verwendet das System die Standardgeschwindigkeit für die von Ihnen für jeden Index gesetzte spezifische Begrenzung.
Hinzufügen	Die spezifische Geschwindigkeitsbegrenzung der obigen Liste hinzufügen.
Bearbeiten	Ermöglicht Ihnen, die Einstellungen der gewählten Begrenzung zu bearbeiten.
Löschen	Gewählte Einstellungen von der Begrenzungsliste entfernen.
Index (1-15) in der Timerkonfiguration	Sie können für Ihre Anforderungen vier Timer einrichten. Alle Timer können im Voraus auf der Web-Seite **Anwendungen – Timer** eingestellt werden, und Sie können die Nummer verwenden, die Sie auf jener Web-Seite gesetzt haben.

4.7.3 QoS

Der Einsatz von QoS (Quality of Service) sorgt dafür, dass alle Anwendungen die erforderliche Dienstgüte und genügend Bandbreite erhalten, um die erwartete Leistung zu erbringen, was zweifellos ein wichtiger Aspekt eines modernen Unternehmensnetzwerks ist.

Ein Grund für den Einsatz von QoS ist, dass viele TCP-basierte Anwendungen ihre Übertragungsgeschwindigkeit im Verlauf der Sitzung erhöhen und dann möglicherweise die gesamte verfügbare Bandbreite in Anspruch nehmen (TCP Slow Start). Ohne QoS-Schutz würde ein großer Teil der Leistung anderer Anwendungen im übervollen Netzwerk verloren gehen. Dies ist besonders für Anwendungen wichtig, die gegenüber Verlusten, Verzögerungen oder Jitter (Laufzeitvarianz) empfindlich sind.

Ein anderer Grund für den Einsatz von QoS liegt in den Engpässen, die an Netzwerkkreuzungen entstehen können, an denen Netzwerkstrecken mit unterschiedlichen Geschwindigkeiten aufeinander treffen oder an denen sich der Verkehr staut und Pakete warten müssen, wodurch der Verkehr auf eine niedrigere Geschwindigkeit gedrosselt werden kann. Falls es keine definierte Priorität gibt, die bestimmt, welche Pakete aus einer überfließenden Warteschlange verworfen werden sollen, könnten Pakete empfindlicher Anwendungen betroffen sein. Wie würde sich dies auf die Leistung der jeweiligen Anwendung auswirken?

Die primäre QoS-Konfiguration beinhaltet zwei Komponenten:

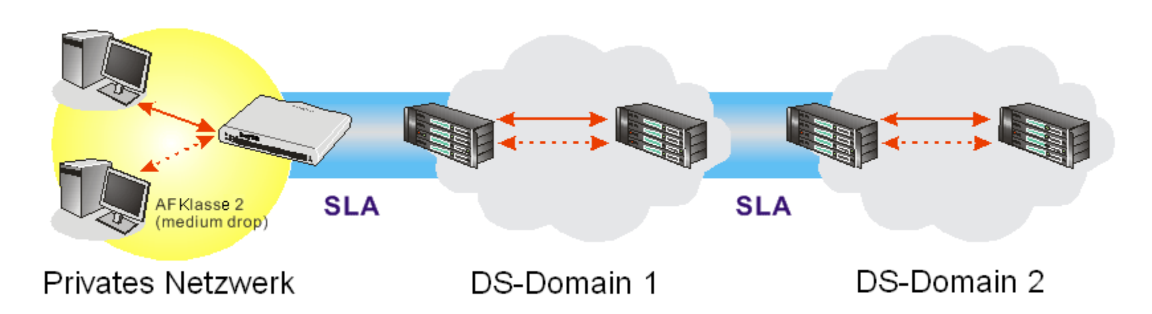
- Klassifizierung: Erkennung von kritischen Anwendungen und Anwendungen mit niedriger Latenz und Kennzeichnung für Dienstgüte mit hoher Priorität im gesamten Netzwerk.
- Zeitplanung: Zuweisung von Paketen zu Warteschlangen und Servicetypen auf der Grundlage der Klassifizierung der Dienstgüte.

Der grundlegende QoS-Ansatz der Vigor-Router besteht darin, Pakete aufgrund der Servicetyp-Information im IP-Header zu klassifizieren und einzuplanen. Um zum Beispiel die Verbindung zur Firmenzentrale zusichern, kann ein Teleworker einen QoS-Kontrollindex bestimmen, um Bandbreite für eine HTTPS-Verbindung zu sichern und gleichzeitig viele andere Anwendungen zu nutzen.

Eine erweiterte Möglichkeit der QoS-Technik besteht in der Verwendung von DSCP (Differentiated Service Code Point) und IP Precedence auf Schicht 3. Im Gegensatz zum herkömmlichen IP Precedence, welches das ToS (Type of Service) Feld im IP-Header verwendet, um acht Dienstklassen zu definieren, ermöglicht der Nachfolger DSCP 64 Klassen, wobei diese Technik mit IP Precendence abwärtskompatibel ist. In

einem QoS-aktivierten Netzwerk oder Differentiated Service (DiffServ oder DS) System sollte der Inhaber der DS-Domain eine Dienstgütevereinbarung (SLA - Service Level Agreement) mit anderen DS-Domaininhabern unterzeichnen, um die Dienstgüte zu definieren, die für den Verkehr von verschiedenen Domains bereitgestellt wird. Dadurch wird jeder DS-Knoten in diesen Domains entsprechend priorisiert. Dies wird als Per-Hop Behavior (PHB) bezeichnet. Die Definition von PHB umfasst Expedited Forwarding (EF), Assured Forwarding (AF) und Best Effort (BE). AF bietet vier Lieferklassen (bzw. Weiterleitungsklassen) und drei Drop-Prioritätsstufen in jeder Klasse.

Als Edge-Router der DS-Domain überprüfen Vigor-Router den markierten DSCP-Wert im IP-Header des passierenden Verkehrs, um der Klassifizierung und Zeitplanung entsprechend Ressourcen zuzuweisen. Die Core-Router im Backbone wenden vor Ausführung die gleiche Überprüfung an, um im gesamten QoS-aktivierten Netzwerk die entsprechende Dienstgüte zu gewährleisten.



Jeder Knoten kann jedoch aufgrund der SLAs zwischen verschiedenen DS-Domaininhabern eine unterschiedliche Betrachtungsweise der Pakete mit hoher Priorität aufweisen. Es ist daher nicht einfach, alleine durch die Bemühungen des Vigor-Routers im gesamten Netzwerk konsequent QoS-Verkehr mit hoher Priorität zu ermöglichen.

Klicken Sie im Menü **Bandbreitenmanagement** auf **QoS**, um die entsprechende Web-Seite zu öffnen.

Bandbreitenmanagement >> Quality of Service

Basiskonfiguration | Auf Werkseinstellungen zurücksetzen |

Status	Bandbreite	Richtung	Gruppe 1	Gruppe 2	Gruppe 3	Andere	UDP-Bandbreiten Begrenzung	
aktiv	--kbit/s/--kbit/s	Raus	25%	25%	25%	25%	inaktiv	Bearbeiten

Gruppenregeln

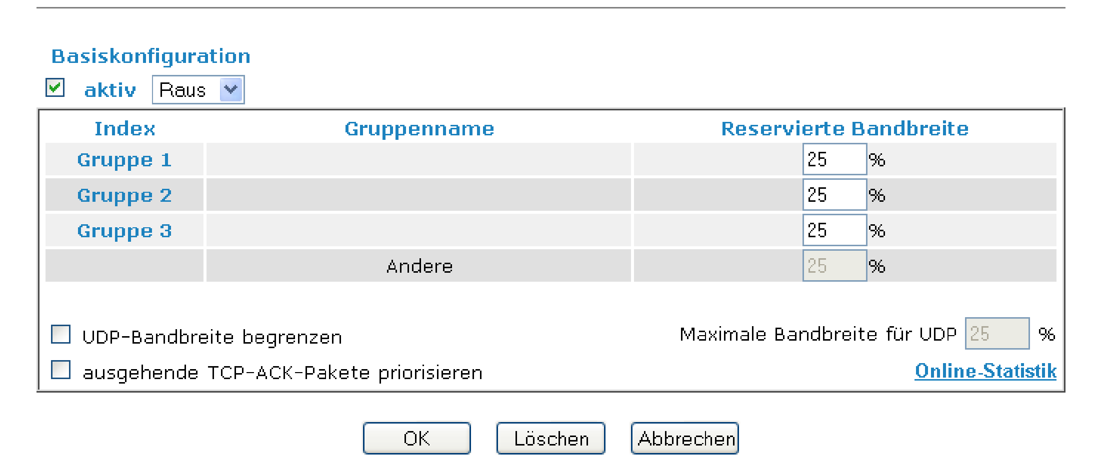
Index	Name	Regel	Servicetyp
Gruppe 1		Ändern	
Gruppe 2		Ändern	Ändern
Gruppe 3		Ändern	

Diese Seite zeigt QoS-Einstellungen der WAN-Schnittstelle an. Klicken Sie auf **Konfiguration**, um für die Basiskonfiguration der WAN-Schnittstelle auf die nächste Seite zu gelangen. Zur Konfiguration der Klassenregeln klicken Sie auf **Bearbeiten**.

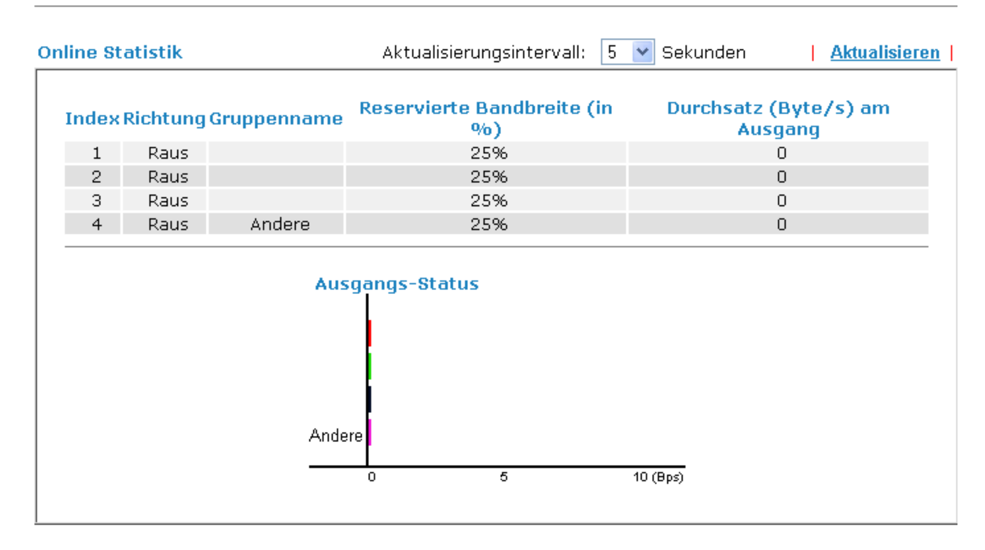
Sie können die Basiskonfiguration der WAN-Schnittstelle, die Klassenregeln und den Servicetyp für die Klassenregeln Ihren Anforderungen entsprechend einrichten.

Basiskonfiguration der WAN-Schnittstelle

Klicken Sie auf **Konfiguration**, um die Bandbreite für QoS der WAN-Schnittstelle zu konfigurieren. Es sind vier Warteschlangen für die QoS-Kontrolle verfügbar. Die ersten drei Klassenregeln (Klasse 1 bis Klasse 3) können Ihren Anforderungen angepasst werden. Die letzte ist für die Pakete reserviert, die nicht für die benutzerdefinierten Klassenregeln geeignet sind.

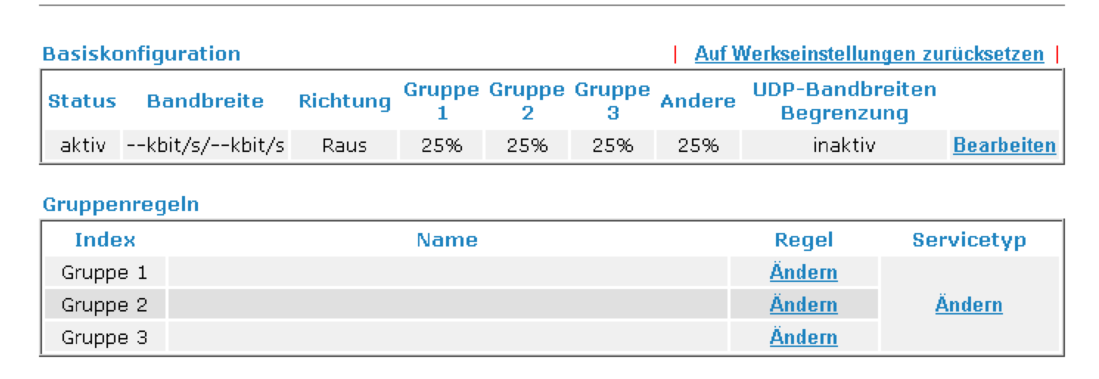


Aktiv	Die Werkseinstellung wird aktiviert. Bitte geben Sie auch an, auf welchen Verkehr die QoS-Einstellungen anzuwenden sind. **Rein -** Nur auf eingehenden Verkehr anwenden. **Raus -** Nur auf ausgehenden Verkehr anwenden. **Beide -** Auf eingehenden und ausgehenden Verkehr anwenden. Markieren Sie das Kästchen und klicken auf **OK**. Dann klicken Sie erneut auf **Konfiguration**. Der Link für **Online-Statistik** erscheint auf dieser Seite.
Reservierte Bandbreite	Wird für den Gruppenindex in Form einer **reservierten Upstream-Bandbreite** und einer **reservierten Downstream-Bandbreite** reserviert.
UDP-Bandbreite begrenzen	Markieren und Bandbreitenbegrenzung im rechten Feld eingeben. Dies stellt einen Schutz für den Verkehr von TCP-Anwendungen dar, da der Verkehr von UDP-Anwendungen wie Streaming Video viel Bandbreite beansprucht.
Ausgehende TCP-ACK-Pakete priorisieren	Der Unterschied zwischen der Download- und Upload-Bandbreite ist in einer ADSL2+-Umgebung beträchtlich. Um zu vermeiden, dass die Download-Geschwindigkeit die Upload-Geschwindigkeit von ausgehenden TCP-ACK-Paketen bremst, markieren Sie dieses Kästchen, um ausgehende ACK-Pakete im Netzwerkverkehr zu beschleunigen.
Maximale Bandbreite für UDP	Der hier eingegebene Wert wird für die maximale Bandbreite von UDP-Anwendungen verwendet.
Online-Statistik	Zeigt eine Online-Statistik der QoS an. Der Link ist nur dann sichtbar, wenn Sie in der Basiskonfiguration für WAN1 auf **OK** klicken und dann erneut unter **Bandbreitenmanagement>>QoS** auf **Konfiguration** (für WAN1) klicken.

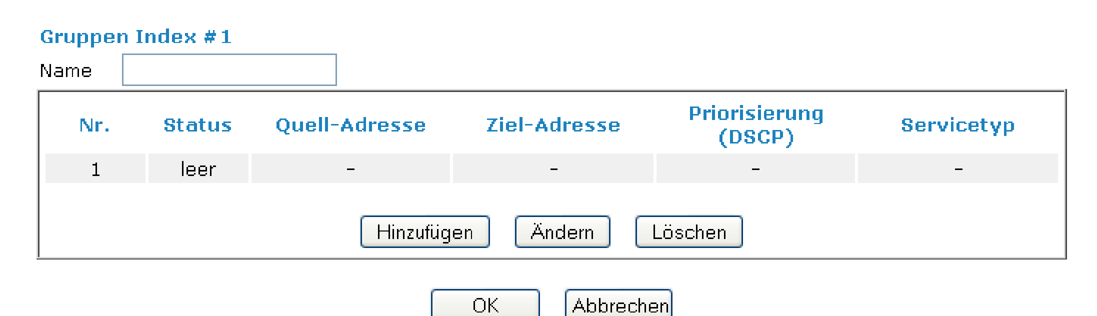


Bearbeiten der Klassenregeln für QoS

Die ersten drei Klassenregeln (Klasse 1 bis Klasse 3) können Ihren Anforderungen angepasst werden. Klicken Sie auf **Bearbeiten**, um eine Klasse hinzuzufügen, zu bearbeiten oder zu löschen.



Wenn Sie auf **Bearbeiten** klicken, sehen Sie die folgende Seite. Sie können nun für die Klasse eine Bezeichnung eingeben. In diesem Fall wird "Test" als Bezeichnung für den Klassenindex Nr. 1 verwendet.



Um eine neue Regel hinzuzufügen, klicken Sie auf **Hinzufügen**, wodurch sich die folgende Seite öffnet.

Bandbreitenmanagement >> Quality of Service

Regel ändern

☑ Aktiv	☐ Hardware-Beschleunigung
Quell-Adresse	Any [Bearbeiten]
Ziel-Adresse	Any [Bearbeiten]
Priorisierung (DSCP)	ANY
Servicetyp	ANY

Hinweis: Bitte konfigurieren/wählen Sie zunächst den Servicetyp !

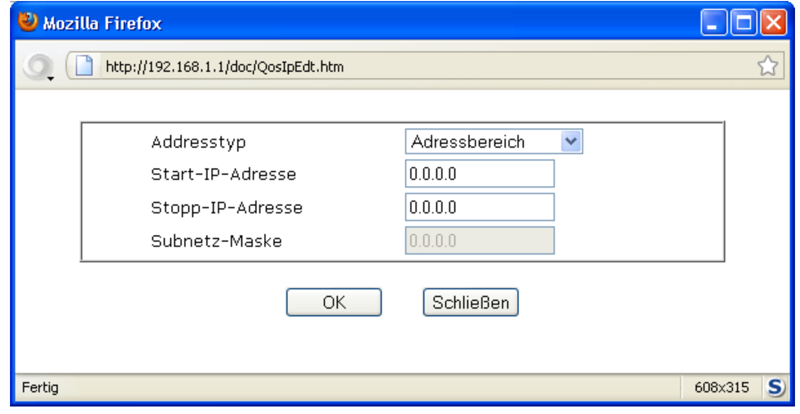
[OK] [Abbrechen]

ACT Markieren Sie dieses Kästchen, um diese Einstellungen zu aktivieren.

Quell-Adresse Klicken Sie auf **Bearbeiten**, um die lokale IP-Adresse (im LAN) für die Regel zu setzen.

Ziel-Adresse Klicken Sie auf **Bearbeiten**, um die entfernte IP-Adresse (im LAN/WAN) für die Regel zu setzen.

Bearbeiten Hier können Sie die Quell-Adresse bearbeiten.



Adresstyp – Bestimmen Sie den Adresstyp der Quell-Adresse.

Für eine **Einzelne Adresse** füllen Sie das Feld für die Start-IP aus.

Für einen **Adressbereich** geben Sie die Start-IP und die End-IP ein.

Für eine **Subnetz-Adresse** füllen Sie die Felder für die Start-IP und Subnetz-Maske aus.

Priorisierung (DSCP) Alle Datenpakete werden unterschiedlich eingestuft und vom System entsprechend verarbeitet. Bitte weisen Sie den Daten für die Verarbeitung mit QoS-Kontrolle eine Stufe zu.

Servicetyp Bestimmt den Servicetyp der Daten für die Verarbeitung mit QoS-Kontrolle. Dieser kann auch bearbeitet werden. Sie können einen vordefinierten Servicetyp aus der Dropdown-Liste der Servicetypen wählen. Diese Typen werden ab Werk vordefiniert. Wählen Sie einfach denjenigen, der vom aktuellen QoS verwendet werden soll.

Sie können je Klasse bis zu 20 Regeln einrichten. Um eine bestehende Regel zu bearbeiten, wählen Sie bitte den entsprechenden Eintrag und klicken auf **Bearbeiten**, um die Seite für die Änderung der Regel zu öffnen.

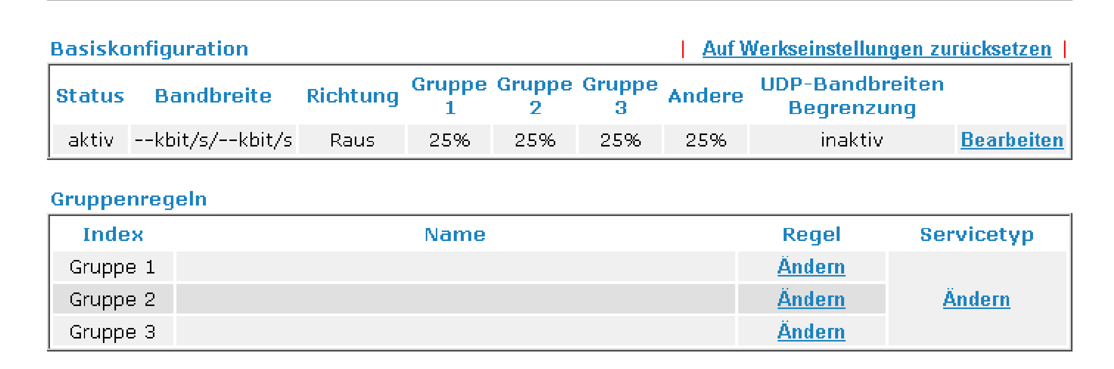
Bearbeiten der Servicetypen für die Klassenregeln

Bandbreitenmanagement >> Quality of Service



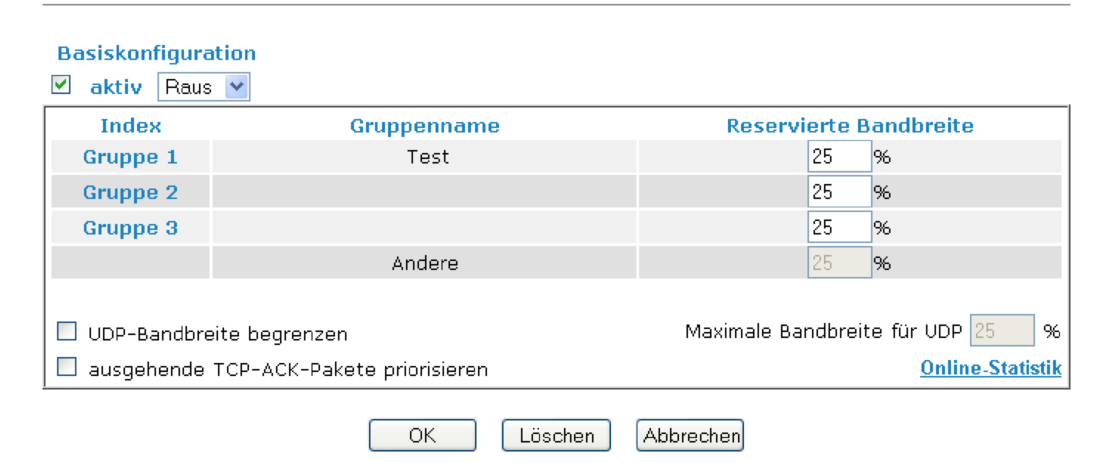
Bitte klicken Sie unter Servicetyp auf Konfiguration, um einen Servicetyp hinzuzufügen, zu bearbeiten oder zu entfernen.

Bandbreitenmanagement >> Quality of Service

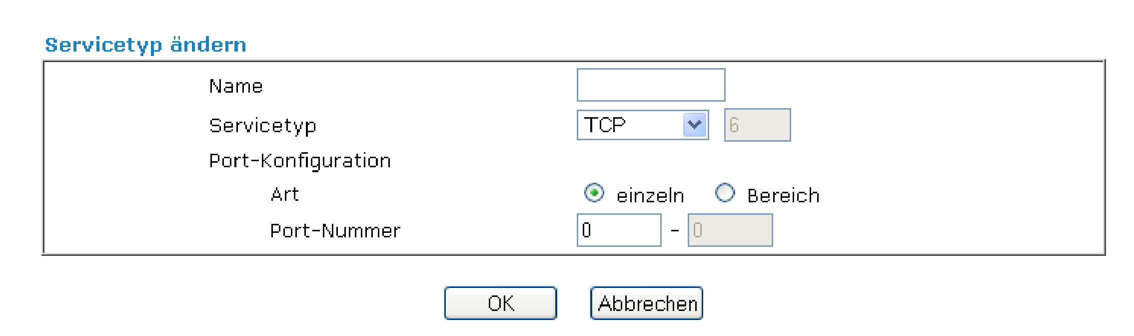


Wenn Sie auf **Bearbeiten** klicken, sehen Sie die folgende Seite:

Bandbreitenmanagement >> Quality of Service



Um einen neuen Servicetyp hinzuzufügen, klicken Sie auf **Hinzufügen**, wodurch sich die folgende Seite öffnet.

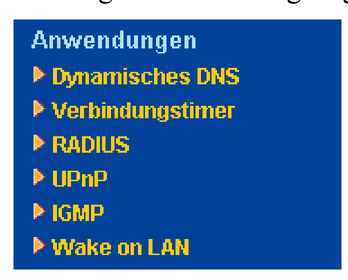


Bezeichnung	Geben Sie Ihren Bedürfnissen entsprechend einen neuen Service ein.
Servicetyp	Wählen Sie den Typ (TCP, UDP oder TCP/UDP) für den neuen Dienst.
Port-Konfiguration	Wählen Sie **Einzeln** oder **Bereich** als **Typ**. Falls Sie Bereich wählen, müssen Sie in den Feldern unten den Start-Port und den End-Port eingeben. **Port-Nummer** – Falls Sie als Typ **Bereich** gewählt haben, geben Sie den Start-Port und den End-Port hier ein.

Sie können bis zu 40 Servicetypen einrichten. Um einen bestehenden Servicetyp zu bearbeiten oder zu löschen, wählen Sie bitte den entsprechenden Eintrag und klicken auf **Bearbeiten**.

4.8 Anwendungen

Die folgende Abbildung zeigt die Menüeinträge für Anwendungen:



4.8.1 Dynamisches DNS

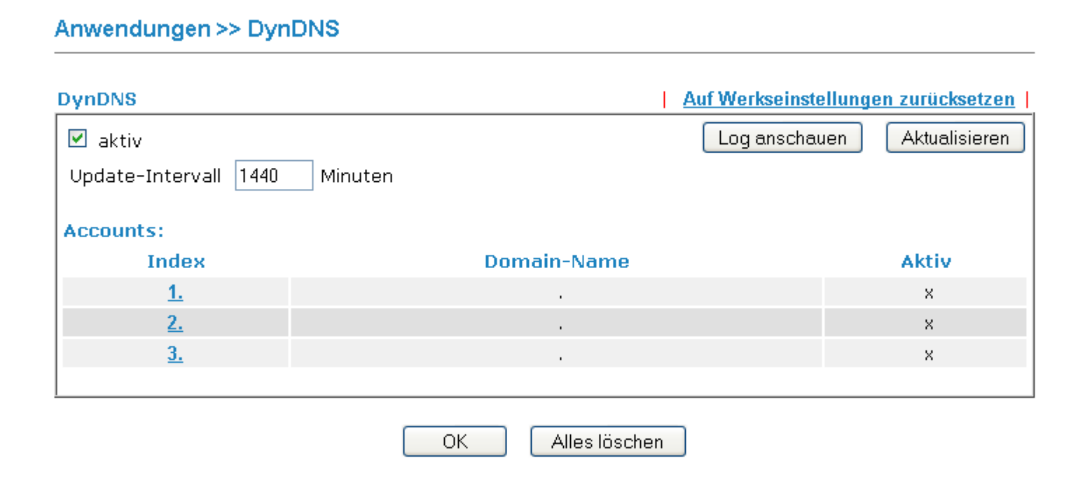
Der ISP weist Ihnen meistens eine dynamische IP-Adresse zu, mit der Sie sich über Ihren ISP mit dem Internet verbinden können. Dies bedeutet, dass sich die Ihrem Router zugewiesene öffentliche IP-Adresse in gewissen Abständen ändert. Die dynamische DNS-Funktion ermöglicht Ihnen, einer dynamischen WAN-IP-Adresse einen Domain-Namen zuzuweisen. So kann der Router seine Online-WAN-IP-Adresszuweisungen auf dem angegebenen DDNS-Server aktualisieren. Wenn der Router online ist, ist es möglich, anhand des registrierten Domain-Namens aus dem Internet auf den Router oder auf die internen virtuellen Server zuzugreifen. Dies ist besonders dann sinnvoll, wenn Sie hinter dem Router einen Web-Server, FTP-Server oder andere Server betreiben.

Bevor Sie die dynamische DNS-Funktion nutzen können, müssen Sie vom DDNS-Anbieter die Freischaltung des DDNS-Dienstes beantragen. Der Router ermöglicht die Einrichtung von bis zu drei Konten bei drei verschiedenen DDNS-Anbietern. Grundsätzlich sind Vigor-Router mit den DDNS-Diensten der beliebtesten DDNS-Anbieter kompatibel, z.B. **www.dyndns.org, www.no-ip.com, www.dtdns.com, www.changeip.com, www.dynamic-nameserver.com.** Besuchen Sie deren Web-Sites, um Ihren Domain-Namen für den Router zu registrieren.

Funktion aktivieren und dynamisches DNS-Konto hinzufügen

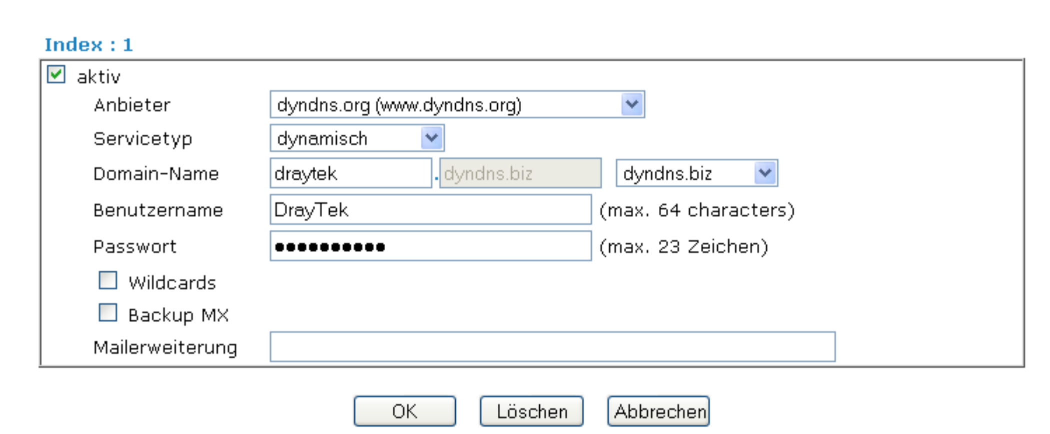
5. Nehmen wir an, der bei Ihrem DDNS-Anbieter registrierte Domain-Name ist *hostname.dyndns.org*, und Sie haben ein Konto mit dem Benutzernamen *test* und dem Passwort *test*.

6. Markieren Sie im DDNS-Konfigurationsmenü den Punkt **Aktiv**.



Auf Werkseinstell-ungen zurücksetzen	Alle Profile löschen und Werkseinstellungen wiederherstellen.
Aktiv	Markieren Sie dieses Kästchen, um die DDNS-Funktion zu aktivieren.
Index	Klicken Sie auf eine Nummer unter Index, um auf die DDNS-Konfigurationsseite zu gelangen.
Domain-Name	Domain-Namen anzeigen, den Sie auf der Seite mit den DDNS-Einstellungen eingegeben haben.
Aktiv	Anzeigen, ob dieses Konto aktiv oder inaktiv ist.
Log ansehen	DDNS-Log-Status anzeigen.
Aktualisieren	Zwingt den Router, seine Information mit dem DDNS-Server zu aktualisieren.

7. Wählen Sie Indexnummer 1, um ein Konto für den Router hinzuzufügen. Markieren Sie **Aktiv**, wählen Sie dyndns.org als Anbieter und geben Sie den registrierten Hostnamen *hostname* und den Domain-Namenssuffix dyndns.org unter **Domain-Name** ein. In den folgenden Feldern geben Sie Ihren Benutzernamen und das Passwort ein.



Aktiv	Markieren Sie dieses Kästchen, um das aktuelle Konto zu aktivieren. Wenn Sie dieses Kästchen aktiviert haben, erscheint in der Spalte "Aktiv" auf der vorherigen Web-Seite von Schritt 2. ein Häkchen.
WAN-Schnittstelle	Wählen Sie die WAN-Schnittstelle, auf welcher die Einstellungen angewendet werden sollen.
Anbieter	Wählen Sie den Anbieter für das DDNS-Konto
Servicetyp	Wählen Sie einen Servicetyp (dynamisch, benutzerdefiniert oder statisch). Falls Sie "benutzerdefiniert" wählen, können Sie die Domain ändern, die im Feld "Domain-Name" gewählt ist.
Domain-Name	Geben Sie einen Domain-Namen ein, den Sie zuvor konfiguriert haben. Verwenden Sie die Dropdown-Liste, um die gewünschte Domain zu wählen.
Benutzername	Geben Sie den Benutzernamen ein, den Sie für die Domain konfiguriert haben.
Passwort	Geben Sie das Passwort ein, das Sie für die Domain gesetzt haben.

8. Klicken Sie auf **OK**, um die Einstellungen zu aktivieren. Ihre Einstellungen werden gespeichert.

Die Wildcard- und Backup MX-Funktionen werden nicht von allen DDNS-Anbietern unterstützt. Weitere Informationen sind auf den entsprechenden Web-Sites der Anbieter verfügbar.

Funktion deaktivieren und alle dynamischen DNS-Konten löschen

Entfernen Sie im DDNS-Konfigurationsmenü die Markierung von **Aktiv** und klicken Sie auf **Alle löschen**, um die Funktion zu deaktivieren und alle Konten vom Router zu löschen.

Ein dynamisches DNS-Konto löschen

Klicken Sie im DDNS-Konfigurationsmenü auf die **Index**nummer, die Sie löschen möchten, und klicken Sie auf **Löschen**, um das Konto zu löschen.

4.8.2 Verbindungstimer

Der Vigor-Router verfügt über eine Echtzeituhr, die manuell oder automatisch über NTP (Network Time Protocol) aktualisiert werden kann. So können Sie nicht nur die Zeiten bestimmen, zu denen der Router eine Verbindung mit dem Internet aufbauen soll, sondern auch den Zugang zum Internet so beschränken, dass Benutzer nur zu bestimmten Zeiten (z.B. Öffnungszeiten) Zugriff auf das Internet haben. Der Timer kann auch für andere Funktionen verwendet werden.

Vor Einrichtung des Timers müssen Sie die Uhrzeit richtig einstellen. Klicken Sie unter **Systemmanagement>> Zeit und Datum** auf **Zeit abrufen**, um die Uhr des Vigor-Routers auf die aktuelle Zeit Ihres Rechners zu setzen. Die Uhr wird zurückgesetzt, wenn Sie den Router ausschalten oder auf die Werkseinstellungen zurücksetzen. Es gibt auch eine andere Methode, um die Uhrzeit abzufragen. Sie können die Router-Zeit mit einem NTP-Server (Zeitserver) im Internet synchronisieren. Allerdings ist dies erst möglich, nachdem eine WAN-Verbindung aufgebaut wurde.

Anwendungen >> Verbindungstimer

Verbindungstimer: | Auf Werkseinstellungen zurücksetzen |

Index	Status	Index	Status
1.	x	9.	x
2.	x	10.	x
3.	x	11.	x
4.	x	12.	x
5.	x	13.	x
6.	x	14.	x
7.	x	15.	x
8.	x		

Status: v --- Aktiv, x --- Inaktiv

Auf Werkseinstellungen zurücksetzen	Alle Profile löschen und Werkseinstellungen wiederherstellen.
Index	Klicken Sie auf eine Nummer unter Index, um auf die Timer-Konfigurationsseite zu gelangen.
Status	Zeigt an, ob dieser Timer aktiv oder inaktiv ist.

Sie können bis zu 15 Timer einrichten. Diese können daraufhin auf die Einstellungen unter **Einwahl ins Internet** oder **VPN und externe Einwahl >> LAN-zu-LAN** angewendet werden.

Um einen Timer hinzuzufügen, klicken Sie auf einen beliebigen Index, z.B. Index Nr. 1. Die Einstellungen des Verbindungstimers unter Index 1 werden in der folgenden Abbildung detailliert dargestellt.

Anwendungen >> Verbindungstimer

Index-Nr. 1

aktiv
Anfangsdatum (yyyy-mm-dd) 2009 - 1 - 1
Startzeit (hh:mm) 0 : 0
Dauer (hh:mm) 0 : 0
Aktion Verbindung aufbauen
Max. Leerlaufzeit 0 Minute(n) - max. 255, 0 ist voreingestellt
Wiederholungen
einmalig
wochentags
So Mo Di Mi Do Fr Sa

OK Löschen Abbrechen

Aktiv	Markieren Sie dieses Kästchen, um den Timer zu aktivieren.
Anfangsdatum (yyyy-mm-dd)	Anfangsdatum des Timers angeben.
Startzeit (hh:mm)	Startzeit des Timers angeben.
Dauer (hh:mm)	Geben Sie die Dauer (oder den Zeitraum) für den Timer an.
Aktion	Geben Sie die Aktion an, die der Verbindungstimer während des Timer-Zeitraums ausführen soll. **Verbindung aufbauen -**Verbindung ständig aufrecht erhalten. **Verbindung beenden -** Verbindung ständig inaktiv halten. **Einwahl zulassen -** Erlauben Sie den Verbindungsaufbau bei Bedarf und geben Sie die Zeit, nachdem die Verbindung abgebrochen werden soll, unter **Max. Leerlaufzeit** an. **Einwahl unterbinden -** Erhält die Verbindung aufrecht, solange über die Leitung Datenaustausch stattfindet. Nach der maximalen Leerlaufzeit ohne Datenaustausch wird die Verbindung abgebrochen und die erneute Einwahl während des Timer-Zeitraums unterbunden.
Max. Leerlaufzeit	Geben Sie die Dauer (oder den Zeitraum) für den Timer an. **Wiederholungen -** Geben Sie an, wie oft der Timer wiederholt werden soll. **Einmalig -** Der Timer kommt nur einmal zur Anwendung. **Wochentags -** Geben Sie die Wochentage an, an denen der Zeitplan angewendet werden soll.

Beispiel

Angenommen, Sie möchten, dass die PPPoE-Internetverbindung während der ganzen Woche von 9:00 Uhr bis 18:00 aktiv ist. Zu anderen Zeiten soll die Internetverbindung nicht aktiv sein (Verbindung beenden).

Bürozeit: **(Verbindung aufbauen)**			
Mo - So	**9:00 Uhr**	**bis**	**18:00 Uhr**

1. Die PPPoE-Verbindung muss ordnungsgemäß funktionieren und **Zeit und Datum** müssen richtig eingestellt sein.
2. Richten Sie das System so ein, dass PPPoE jeweils die ganze Woche von 9:00 bis 18:00 verfügbar ist.
3. Konfigurieren Sie die Aktion **Verbindung beenden** so, dass die Verbindung während der ganzen Woche von 18:00 Uhr bis zum nächsten Tag um 9:00 Uhr nicht verfügbar ist.
4. Weisen Sie diese beiden Profile dem PPPoE-Internet-Einwahlprofil zu. Der Router wird gemäß den voreingestellten Timer-Profilen die **Verbindung aufbauen** oder die **Verbindung beenden**.

4.8.3 RADIUS

RADIUS (Remote Authentication Dial-In User Service) ist ein Client-Server-Protokoll, das zur sicheren Authentifizierung, Autorisierung und zum Accounting dient, und wird von vielen ISPs verwendet. Es ist die am weitesten verbreitete Methode für die Authentifizierung und Autorisierung von Einwahl- und Tunnelverbindungen von Netzwerkbenutzern.

Die eingebaute RADIUS Client-Funktionalität ermöglicht dem Router, den externen Benutzer oder einen WLAN-Client und den RADIUS-Server bei der gegenseitigen Authentifizierung zu unterstützen. Die Funktionalität ermöglicht zentralisierte Fernzugriffsauthentifizierung für Netzwerkmanagement.

Anwendungen >> RADIUS

RADIUS-Einstellungen

☑ aktiv	
Server-IP	
Ziel-Port	1812
Shared Secret	
Shared Secret bestätigen	

OK Löschen Abbrechen

Aktiv	Markieren Sie dieses Kästchen, um die RADIUS-Client-Funktionalität zu aktivieren.
Server-IP	Geben Sie die IP-Adresse des RADIUS-Servers ein.
Ziel-Port	Die vom RADIUS-Server verwendete UDP-Port-Nummer. Der Standardwert gemäß RFC 2138 ist 1812.
Shared Secret	Der RADIUS-Server und der Client teilen sich ein Geheimnis (Secret) mit, das verwendet wird, um die zwischen ihnen kommunizierten Meldungen zu authentifizieren. Beide Seiten müssen so konfiguriert werden, dass sie das gleiche Shared Secret verwenden.
Shared Secret bestätigen	Bestätigen Sie das Shared Secret durch erneute Eingabe.

4.8.4 UPnP

Das **UPnP**-Protokoll (Universal Plug and Play) wird unterstützt, um die Installation und Konfiguration von Netzwerkgeräten zu vereinfachen, wie dies bereits bei direkt angeschlossenen PC-Peripheriegeräten mit dem Windows "Plug and Play"-System der Fall ist. Bei NAT-Routern ist "NAT-Traversal" die wichtigste UPnP-Funktion des Routers. Sie ermöglicht Anwendungen hinter der Firewall, automatisch die Ports zu öffnen, die für die Weiterleitung durch einen Router erforderlich sind. Dies ist verlässlicher, als den Router selbst feststellen zu lassen, welche Ports geöffnet werden müssen. Außerdem muss der Benutzer keine Port-Zuordnungen oder DMZ manuell einrichten. **UPnP ist für Windows XP verfügbar**, und der Router bietet die entsprechende Unterstützung für MSN Messenger, um die Verwendung der Sprach-, Video- und Messaging-Funktionen uneingeschränkt zu ermöglichen.

Anwendungen >> UPnP

UPnP

☑ aktiv

☐ Dienst für die Verbindungskontrolle aktivieren

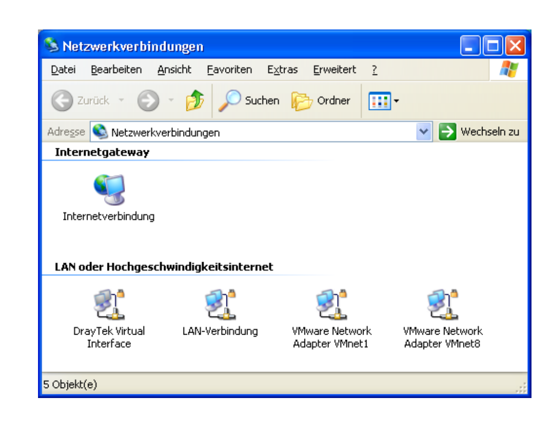
☐ Dienst für den Verbindungsstatus aktivieren

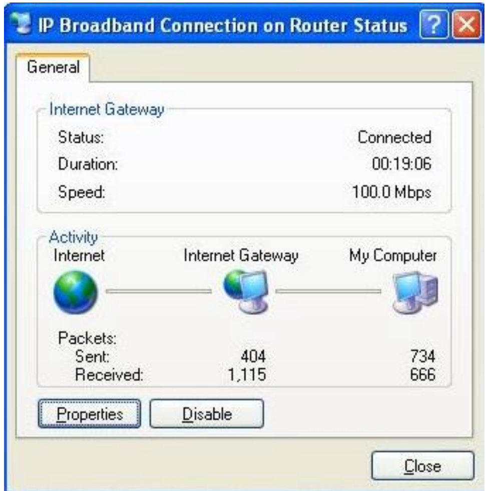
Hinweis: Bei aktivem UPnP kann der Router aus dem LAN heraus veranlasst werden, verschiedene Ports zu öffnen. Es könnten Sicherheitslücken in den NAT- und Firewall-Einstellungen entstehen, weshalb UPnP nur mit Bedacht aktiviert werden sollte.

OK | Löschen | Abbrechen

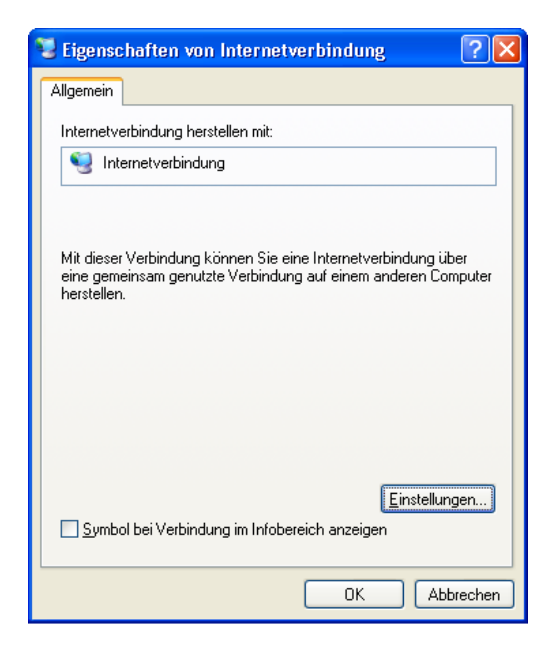
Aktiv Sie können entweder den Dienst für die **Verbindungskontrolle** oder den Dienst für den **Verbindungsstatus** aktivieren.

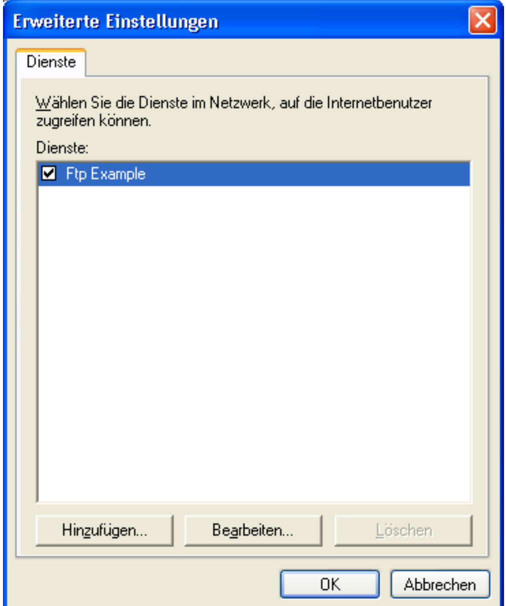
Nachdem diese Funktion auf **Aktiv** gesetzt wurde, erscheint unter Windows XP/Netzwerkverbindungen das Symbol **IP-Breitbandverbindung auf Router**. Der Verbindungsstatus und der Verbindungskontrollstatus können aktiviert werden. Die NAT-Traversal-Funktion von UPnP ermöglicht die Verwendung der Multimedia-Funktionen Ihrer Anwendungen. Die Port-Zuordnungen müssen manuell oder anderweitig eingestellt werden. Die folgenden Screenshots zeigen anhand von Beispielen, wie dies funktioniert.





Die UPnP-Funktion des Routers ermöglicht Anwendungen mit UPnP-Unterstützung wie MSN Messenger, zu erkennen, was sich hinter einem NAT-Router befindet. Die Anwendung erkennt auch die externe IP-Adresse und konfiguriert die Port-Zuordnungen auf dem Router. Danach ermöglicht diese Funktion die Weiterleitung von Paketen von den externen Ports des Routers zu den internen Ports, die von der Anwendung verwendet werden.





Hinweis zur Firewall und UPnP

Probleme mit Firewall-Software
Der Einsatz von Firewall-Anwendungen auf Ihrem Rechner kann die UPnP-Funktion behindern. Dies liegt daran, dass diese Anwendungen den Zugriff auf einige Netzwerk-Ports blockieren.

Sicherheitsüberlegungen
Die Verwendung der UPnP-Funktion in Ihrem Netzwerk kann gewisse Sicherheitsrisiken mit sich bringen. Sie sollten diese Risiken genau abwägen, bevor Sie die UPnP-Funktion aktivieren.

- Da die Schwächen der UPnP-Funktion bei manchen Microsoft-Betriebssystemen ausgenutzt werden können, ist es wichtig, die neuesten Service Packs und Patches einzuspielen.
- Nicht privilegierte Benutzer können gewisse Router-Funktionen steuern, z.B. Port-Zuordnungen entfernen und hinzufügen.

Die UPnP-Funktion fügt dynamisch Port-Zuordnungen für einige Anwendungen mit UPnP-Unterstützung hinzu. Falls diese Anwendungen abstürzen, kann es sein, dass diese Zuordnungen nicht entfernt werden.

4.8.5 IGMP

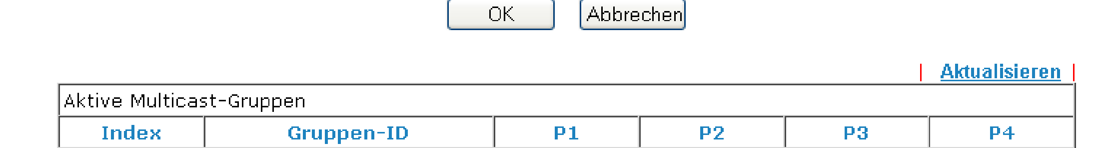
IGMP ist die Abkürzung für *Internet Group Management Protocol*. Es handelt sich hierbei um ein Kommunikationsprotokoll, das hauptsächlich für die Verwaltung der Mitgliedschaft in Internet-Protokoll-Multicast-Gruppen zum Einsatz kommt.

Anwendungen >> IGMP

IGMP

☐ IGMP-Proxy aktiv
Der IGMP-Proxy agiert als Multicast-Proxy für Hosts im LAN. Aktivieren Sie diesen, wenn Sie Zugang zu Multicast-Gruppen wünschen. Diese Funktion erzielt **keinen Effekt bei aktivem Bridge-Modus**.

☐ IGMP-Snooping aktiv
Aktivieren Sie IGMP-Snooping, damit Multicasts nur an Ports weitergeleitet werden, an welchen sich Mitglieder der entsprechenden Gruppe befinden.
Ist IGMP-Snooping inaktiv, so werden Multicasts genau wie Broadcasts behandelt.



IGMP-Proxy aktiv Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Die Multicast-Anwendung wird über den WAN-Port ausgeführt.

IGMP-Snooping aktiv Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren. Der Multicast-Traffic wird an Ports weitergeleitet, welche über Mitglieder der Gruppe verfügen. Wird IGMP-Snooping deaktiviert, so wird der Multicast-Traffic genau wie Broadcast-Traffic behandelt.

Gruppen-ID Dieses Feld zeigt den ID-Port für die Multicast-Gruppe an. Der verfügbare Bereich für IGMP reicht von 224.0.0.0 bis 255.255.254.

P1 bis P4 Zeigt den LAN-Port an, der für die Multicast-Gruppe verwendet wird.

Aktualisieren Klicken Sie hier, um den Status der Multicast-Gruppe zu aktualisieren.

Wenn Sie IGMP-Proxy aktiv markieren, werden alle Multicast-Gruppen und alle verfügbaren LAN-Ports (P1 bis P4) aufgeführt.

4.8.6 Wake on LAN

Ein mit dem LAN verbundener Rechner kann vom Router aufgeweckt werden. Um einen bestimmten Rechner über den Router aufzuwecken, muss die korrekte MAC-Adresse des jeweiligen Rechners auf dieser Web-Seite angegeben werden.

Außerdem muss der Rechner über eine Netzwerkkarte verfügen, welche die WOL-Funktion unterstützt. Die WOL-Funktion muss im BIOS des jeweiligen Rechners aktiviert werden.

Anwendungen >> Wake on LAN

Wake on LAN

Hinweis: Wake on LAN arbeitet mit IP an MAC binden zusammen; nur gebundene PCs können durch ihre IP-Adresse geweckt werden.

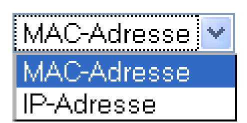
Wecken durch: MAC-Adresse

IP-Adresse:

MAC-Adresse: [ ]:[ ]:[ ]:[ ]:[ ]:[ ] Aufwecken!

Ergebnis

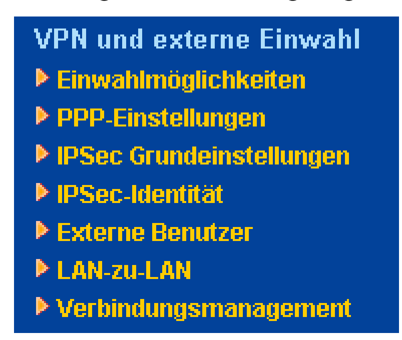
ddns time <update in minutes>Valid: 1 ~ 1440Now: 1440

Wecken durch:	Ein Gerät kann auf zweierlei Weise aufgeweckt werden. Falls Sie Wecken durch MAC-Adresse wählen, müssen Sie die korrekte MAC-Adresse des Hosts im MAC-Adressfeld eingeben. Falls Sie Wecken durch IP-Adresse wählen, müssen Sie die richtige IP-Adresse bestimmen. 
IP-Adresse	Die IP-Adressen, die unter **Firewall>>IP an MAC binden** vorhanden sind, erscheinen in dieser Dropdown-Liste. Wählen Sie die IP-Adresse, welche Sie aufwecken möchten, aus der Dropdown-Liste.
MAC-Adresse	Geben Sie die MAC-Adresse eines gebundenen PCs an.
Aufwecken!	Klicken Sie auf diese Taste, um die ausgewählte IP aufzuwecken. Sehen Sie die folgende Abbildung. Das Ergebnis wird im Feld angezeigt.

4.9 VPN und externe Einwahl

Ein VPN (Virtual Private Network) ist die Erweiterung eines privaten Netzwerks, dass Verbindungen über gemeinsame bzw. öffentliche Netzwerke wie das Internet ermöglicht. Die Übertragung von Daten zwischen zwei Rechnern über ein gemeinsames bzw. öffentliches Netzwerk mit der VPN-Technologie entspricht den Eigenschaften einer privaten P2P-Verbindung.

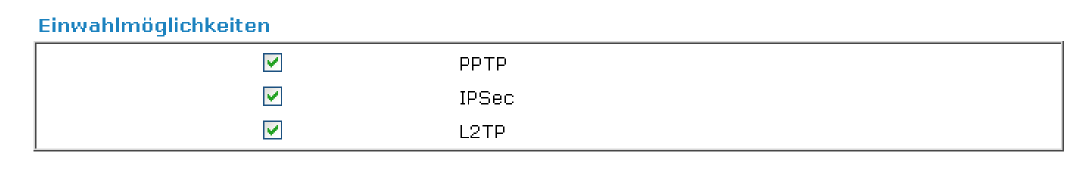
Die folgende Abbildung zeigt die Menüeinträge für VPN und Fernzugriff:



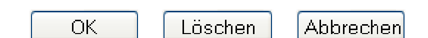
4.9.1 Einwahlmöglichkeiten

Aktivieren Sie bei Bedarf den erforderlichen VPN-Dienst. Falls Sie beabsichtigen, in Ihrem LAN einen VPN-Server zu betreiben, sollten Sie den VPN-Dienst des Vigor-Routers deaktivieren, damit die Datenpakete den VPN-Tunnel passieren können, und die entsprechenden NAT-Einstellungen vornehmen (DMZ, Ports öffnen).

VPN und externe Einwahl >> Einwahlmöglichkeiten



Hinweis: Wenn Sie einen VPN-Server in Ihrem LAN betreiben wollen, müssen Sie die entsprechenden Protokolle oben deaktivieren. Nur so können die Datenpakete uneingeschränkt passieren. Außerdem sollten Sie die verwendeten Ports für den VPN-Server in den NAT- und Firewall-Einstellungen des Routers öffnen.



4.9.2 PPP-Einstellungen

Dieses Untermenü wird nur für PPP-bezogene VPN-Verbindungen wie PPTP, L2TP und L2TP over IPSec benötigt.

VPN und externe Einwahl >> PPP-Einstellungen

PPP-Einstellungen

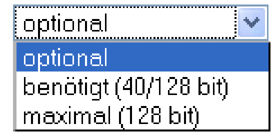
PPP/MP-Protokoll		IP-Adressenzuweisung für die einwählenden Benutzer (wenn DHCP-Server inaktiv)	
PPP-Authentifizierung beim Einwählen	PAP oder CHAP	IP-Adressbereich zuweisen	192.168.1.200
PPP-Verschlüsselung (MPPE) beim Einwählen	optional		
Gegenseitige Authentifizierung (PAP)	○ Ja ⦿ Nein		
Benutzername			
Passwort			

OK

PPP-Authentifizierung beim Einwählen Nur PAP
Wählen Sie diese Option, damit der Router Einwahlbenutzer über das PAP-Protokoll authentifiziert.

PAP oder CHAP
Wählen Sie diese Option, so versucht der Router zunächst, Einwahlbenutzer über das CHAP-Protokoll zu authentifizieren. Falls der Einwahlbenutzer dieses Protokoll nicht unterstützt, wird für die Authentifizierung auf das PAP-Protokoll zurückgegriffen.

PPP-Verschlüsselung (MPPE) beim Einwählen Optional
Wird diese Option gewählt, verwendet der Router optional die MPPE-Verschlüsselungsmethode für externe Benutzer. Falls der externe Benutzer den MPPE-Verschlüsselungsalgorithmus nicht unterstützt, versendet der Router keine MPPE-verschlüsselten Pakete. Ansonsten werden die Daten mit MPPE verschlüsselt.



Benötigt (40/128 bit) - Die Auswahl dieser Option zwingt den Router, Pakete mit dem MPPE-Algorithmus zu verschlüsseln. Der externe Benutzer setzt zunächst 40-Bit-Verschlüsselung ein, bevor 128-Bit-Verschlüsselung zum Einsatz kommt. Falls 128-Bit MPPE-Verschlüsselung nicht verfügbar ist, wird also für die Verschlüsselung der Daten 40-Bit-Verschlüsselung verwendet.

Maximal (128 bit) - Mit dieser Option verwendet der Router die MPPE-Verschlüsselung mit maximaler Bit-Anzahl (128 Bits), um die Daten zu verschlüsseln.

Gegenseitige Authentifizierung (PAP)
Die Funktion zur gegenseitigen Authentifizierung dient hauptsächlich der Kommunikation mit anderen Routern oder Clients, die zweiseitige Authentifizierung erfordern, um ein höheres Sicherheitsniveau zu erreichen (z.B. Cisco-Router). Sie sollten daher diese Funktion aktivieren, falls der andere Router dies erfordert. Geben Sie in diesem Fall den **Benutzernamen** und das **Passwort**

des Peers für die gegenseitige Authentifizierung ein.

Start-IP-Adresse Geben Sie für die PPP-Einwahlverbindung eine Start-IP ein. Wählen Sie eine IP-Adresse aus dem lokalen privaten Netzwerk. Wenn zum Beispiel das lokale private Netzwerk 192.168.1.0/255.255.255.0 ist, können Sie 192.168.1.200 als Start-IP-Adresse wählen.

4.9.3 IPSec Grundeinstellungen

In den **IPSec Grundeinstellungen** besteht die Konfiguration aus zwei wesentlichen Teilen.

IPSec umfasst zwei Phasen:

- Phase 1: Aushandlung von IKE-Parametern wie Verschlüsselung, Hash, Diffie-Hellman-Parameterwerte und Gültigkeitsdauer, um den nachfolgenden IKE-Austausch zu schützen, Authentifizierung beider Peers mit Pre-Shared Key oder digitaler Signatur (x.509). Der Peer, der die Verhandlung initiiert, schlägt dem entfernten Peer alle seine Verfahren vor, und der entfernte Peer versucht, eine Übereinstimmung höchster Priorität zu finden. Schließlich wird ein sicherer Tunnel für IKE Phase 2 eingerichtet.
- Phase 2: Aushandlung von IPSec-Sicherheitsmethoden wie AH (Authentication Header) oder ESP (Encapsulating Security Payload) für den nachfolgenden IKE-Austauch und gegenseitige Prüfung des Aufbaus eines sicheren Tunnels.

Es werden für IPSec zwei Kapselungsmethoden verwendet: **Transport** und **Tunnel**. Der **Transport**-Modus fügt die AH-/ESP-Daten hinzu und benutzt die ursprünglichen IP-Header, um nur die Nutzdaten zu kapseln. Dies ist nur beim lokalen Paket möglich, z.B. L2TP über IPSec. Der **Tunnel**-Modus fügt nicht nur die AH-/ESP-Daten hinzu, sondern verwendet außerdem einen neuen IP-Header (Tunneled IP Header), um das gesamte ursprüngliche IP-Paket zu kapseln.

AH (Authentication Header) bietet Datenauthentifizierung und Integrität für IP-Pakete, die zwischen den VPN-Peers ausgetauscht werden. Zu diesem Zweck wird eine verschlüsselte Einweg-Hash-Funktion auf das Paket angewendet, um einen Message Digest zu erstellen. Dieser Digest wird in den AH integriert und mit den Paketen zusammen übertragen. Auf der Empfängerseite wendet der Peer die gleiche Einweg-Hash-Funktion auf das Paket an und vergleicht den Wert mit dem Wert im empfangenen AH.

ESP (Encapsulating Security Payload) ist ein Sicherheitsprotokoll, dass Vertraulichkeit und Datenschutz mit optionaler Authentifizierung und Replay-Erkennung bietet.

VPN und externe Einwahl >> IPSec Grundeinstellungen

IKE/IPSec Grundeinstellungen

Einstellungen für die Einwahl in diesen Router von außen (LAN-zu-LAN).

IKE-Authentifizierungsmethode

Pre-Shared Key

Pre-Shared Key bestätigen

IPSec-Sicherheitsmethode

☑ Mittel (AH)

Daten werden authentifiziert, aber nicht verschlüsselt.

Hoch (ESP) ☑ DES ☑ 3DES ☑ AES

Daten werden sowohl authentifiziert als auch verschlüsselt.

OK Abbrechen

IKE-Authentifizierungsmethode

Betrifft normalerweise externe Benutzer oder Knoten (LAN zu LAN), die dynamische IP-Adressen und IPSec-bezogene VPN-Verbindungen wie L2TP über IPSec und IPSec-Tunnel benutzen.

Pre-Shared Key - Zur Zeit wird nur Authentifizierung mit Pre-Shared Key unterstützt.

Pre-Shared Key - Geben Sie einen Schlüssel für IKE-Authentifizierung an.

Pre-Shared Key bestätigen - Geben Sie die Zeichenfolge erneut ein, um den Pre-Shared Key zu bestätigen.

IPSec-Sicherheitsmethode

Mittel - Authentication Header (AH) bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig aktiviert.

Hoch - Encapsulating Security Payload (ESP) bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Als Verschlüsselungsalgorithmus stehen DES (Data Encryption Standard), 3DES (Triple DES) und AES zur Verfügung.

4.9.4 IPSec-Identität

Um für die Peer-Authentifizierung bei LAN-zu-LAN-Verbindungen oder externen Einwahlverbindungen digitale Zertifikate zu verwenden, können Sie hier eine Liste von Peer-Zertifikaten verwalten. Wie aus der folgenden Abbildung ersichtlich, bietet der Router **32** Einträge für digitale Zertifikate für Einwahlbenutzer.

VPN und externe Einwahl >> IPSec-Identität

X.509 ID Konten: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Auf Werkseinstellungen zurücksetzen	Klicken Sie auf diese Taste, um alle Einträge zu löschen.
Index	Klicken Sie auf eine Nummer unter Index, um auf die Konfigurationsseite für die IPSec-Identität zu gelangen.
Name	Profilnamen dieses Indexes anzeigen.

Klicken Sie auf die einzelnen Einträge, um jeweils ein digitales Peer-Zertifikat zu bearbeiten. Die Authentifizierung der digitalen Signaturen umfasst drei Sicherheitsstufen. Füllen Sie alle erforderlichen Felder aus, um den externen Peer zu authentifizieren. Die folgenden Erläuterungen werden Ihnen dabei behilflich sein, alle notwendigen Felder auszufüllen.

VPN und externe Einwahl >> IPSec-Identität

Profil-Index : 1

Profilname	???
☐ aktiv	
◉ Akzeptiere jede ID	
○ Akzeptiere Subjekt mit übereinstimmmendem Namen/Wert	
Typ	IP-Adresse
IP	
○ Akzeptiere Subjekt mit Übereinstimmung in gewissen Feldern	
Land (C)	
Bundesland (ST)	
Ort (L)	
Orginisation (O)	
Abteilung (OU)	
Bezeichnung (CN)	
E-Mail (E)	

OK | Löschen | Abbrechen

Profilname	Geben Sie in diesem Feld eine Bezeichnung ein.
Akzeptiere jede ID	Hier klicken, um ungeachtet der Identität jeden Peer zu akzeptieren.
Akzeptiere Subjekt mit übereinstimmendem Namen/Wert	Hier klicken, um ein bestimmtes Feld der digitalen Signatur zu markieren, mit dem der Peer übereinstimmen muss, damit er akzeptiert wird. Das Feld kann die **IP-Adresse, Domain,** oder **E-Mail-Adresse** sein. Je nach gewähltem Typ erscheint das entsprechende Feld und fordert Sie zur Eingabe auf.
Akzeptiere Subjekt mit Übereinstimmung in gewissen Feldern	Hier klicken, um die bestimmten Felder der digitalen Signatur zu markieren, mit dem der Peer übereinstimmen muss, damit er akzeptiert wird. Die Felder umfassen **Country (C), State (ST), Location (L), Organization (O), Organization Unit (OU), Common Name (CN)** und **Email (E)**.

4.9.5 Externe Benutzer

Sie können Fernzugriffe verwalten, indem Sie eine Tabelle der Profile externer Benutzer unterhalten. Diese Tabelle ermöglicht die Authentifizierung von Benutzern, die sich über eine VPN-Verbindung einwählen. Sie können Parameter wie die Peer-ID, Verbindungstyp (VPN-Verbindung einschl. PPTP, IPSec Tunnel und L2TP mit oder ohne IPSec), Sicherheitsmethoden usw. einstellen.

Der Router bietet **32** Zugangskonten für externe Benutzer. Durch die eingebaute RADIUS-Client-Funktion können die Benutzerkonten auch für den RADIUS-Server verwendet werden. Die folgende Abbildung zeigt eine Zusammenfassung.

VPN und externe Einwahl >> Externe Benutzer

Profile externer Benutzer: | Auf Werkseinstellungen zurücksetzen |

Index	Benutzer	Status	Index	Benutzer	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Auf Werkseinstellungen zurücksetzen	Klicken Sie auf diese Taste, um alle Einträge zu löschen.
Index	Klicken Sie auf eine Nummer unter Index, um auf die Konfigurationsseite für externe Benutzer zu gelangen.
Benutzer	Zeigt den Benutzernamen des entsprechenden externen Benutzers im LAN-zu-LAN-Profil an. Die Zeichen **???** lassen erkennen, dass das Profil leer ist.
Status	Zeigt den Zugangsstatus des jeweiligen externen Benutzers an. "V" zeigt an, dass der externe Benutzer aktiv ist, während "X" anzeigt, dass er inaktiv ist.

Klicken Sie auf eine der Indexnummern, um ein externes Benutzerprofil zu bearbeiten. **Füllen Sie für jeden Einwahltyp die entsprechenden Felder rechts aus.** Ausgegraute Felder brauchen nicht ausgefüllt zu werden. Die folgenden Erläuterungen werden Ihnen dabei behilflich sein, alle notwendigen Felder auszufüllen.

VPN und externe Einwahl >> Externe Benutzer

Index-Nr. 1

Benutzerkonto und Authentifizierung
☐ aktiv
Max. Leerlaufzeit 300 Sekunden

Einwahl zulassen über
☑ PPTP
☑ IPSec
☑ L2TP mit IPSec ohne

☐ Fernzugriff definieren
IP oder ISDN-Nummer von entferntem Benutzer
oder Peer-ID
NetBIOS-Name durchlassen ◉ ja ○ nein

Benutzername ???
Passwort

IKE-Authentifizierungsmethode
☑ Pre-Shared Key
IKE Pre-Shared Key
☐ Digitale Signatur (X.509)
ohne

IPSec-Sicherheitsmethode
☑ Mittel (AH)
Hoch (ESP) ☑ DES ☑ 3DES ☑ AES
Local ID (optional)

OK Löschen Abbrechen

Aktiv Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren.

Max. Leerlaufzeit - Wenn die Verbindung des externen Benutzers länger als die maximale Leerlaufzeit keine Aktivität aufweist, bricht der Router die Verbindung ab. Standardmäßig beträgt die maximale Leerlaufzeit 300 Sekunden.

PPTP Dem externen Benutzer erlauben, über das Internet eine PPTP VPN-Verbindung aufzubauen. Richten Sie den Benutzernamen und das Passwort des externen Benutzers unten ein.

IPSec-Tunnel Dem externen Benutzer erlauben, über das Internet eine IPSec VPN-Verbindung aufzubauen.

L2TP Dem externen Benutzer erlauben, über das Internet eine L2TP VPN-Verbindung aufzubauen. Sie können L2TP entweder alleine oder zusammen mit IPSec wählen. Treffen Sie die Auswahl wie folgt:

Ohne - IPSec Policy nicht anwenden. Die VPN-Verbindung über L2TP ohne IPSec kann daher als reine L2TP-Verbindung betrachtet werden.

Falls vorhanden - Die IPSec Policy wird nur angewendet falls sie beim Verbindungsaufbau vorhanden ist. Ansonsten wird die Einwahl-VPN-Verbindung eine reine L2TP-Verbindung.

Erforderlich - Geben Sie die IPSec Policy an, die auf jeden Fall für die L2TP-Verbindung erforderlich ist.

Benutzername Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.

Passwort Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.

IKE-Authentifizierungsmethode	Diese Felder werden für IPSec-Tunnel und L2TP mit IPSec verwendet, wenn Sie die IP-Adresse des entfernten Knoten angeben. Die einzige Ausnahme ist die digitale Signatur (X.509), welche bei Auswahl des IPSec-Tunnels unter Angabe oder ohne Angabe der IP-Adresse des entfernten Knoten gesetzt werden kann. **Pre-Shared Key -** Markieren Sie das Kästchen für den Pre-Shared Key, um diese Funktion zu aktivieren, und geben Sie die erforderlichen Zeichen (1-63) als Pre-Shared Key ein. **Digitale Signatur (X.509) –** Markieren Sie das Kästchen für digitale Signatur, um diese Funktion zu aktivieren, und wählen Sie eines der vordefinierten Profile, das unter **VPN und externe Einwahl >>IPSec-Identität** eingerichtet wurde.
IPSec-Sicherheitsmethode	Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec notwendig, wenn Sie den entfernten Knoten angeben. Markieren Sie die Kästchen für das Medium, DES, 3DES oder AES als Sicherheitsmethode.
Mittel	**Authentication Header (AH)** bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig angehakt. Sie können die Option deaktivieren, indem Sie das Häkchen entfernen. **Hoch - Encapsulating Security Payload (ESP)** bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Als Verschlüsselungsalgorithmus stehen DES (Data Encryption Standard), 3DES (Triple DES) und AES zur Verfügung. **Lokale ID -** Geben Sie eine lokale ID an, die für die Einwahleinstellungen im LAN-zu-LAN-Profil zu verwenden ist. Dieser Punkt ist optional und kommt nur im IKE Aggressive Mode zur Anwendung.

4.9.6 LAN zu LAN

Hier können Sie LAN-zu-LAN-Verbindungen verwalten, indem Sie eine Tabelle verschiedener Verbindungsprofile unterhalten. Sie können Parameter wie die Verbindungsrichtung (Einwahl oder Anwahl), die Peer-ID, Verbindungstyp (VPN-Verbindung einschl. PPTP, IPSec Tunnel und L2TP mit oder ohne IPSec), Sicherheitsmethoden usw. einstellen.

Der Router unterstützt zwei VPN-Tunnel und bietet bis zu **32** Profile gleichzeitig. Die folgende Abbildung zeigt eine Zusammenfassung.

VPN und externe Einwahl >> LAN-zu-LAN

LAN-zu-LAN Profile: | Auf Werkseinstellungen zurücksetzen |

Index	Name	Status	Index	Name	Status
1.	???	X	17.	???	X
2.	???	X	18.	???	X
3.	???	X	19.	???	X
4.	???	X	20.	???	X
5.	???	X	21.	???	X
6.	???	X	22.	???	X
7.	???	X	23.	???	X
8.	???	X	24.	???	X
9.	???	X	25.	???	X
10.	???	X	26.	???	X
11.	???	X	27.	???	X
12.	???	X	28.	???	X
13.	???	X	29.	???	X
14.	???	X	30.	???	X
15.	???	X	31.	???	X
16.	???	X	32.	???	X

Auf Werkseinstellungen zurücksetzen	Klicken Sie auf diese Taste, um alle Einträge zu löschen.
Name	Geben Sie den Namen des LAN-zu-LAN-Profils ein. Die Zeichen **???** lassen erkennen, dass das Profil leer ist.
Status	Zeigt den Status einzelner Profile an. "V" zeigt an, dass das Profil aktiv ist, während "X" anzeigt, dass es inaktiv ist.

Klicken Sie auf eine der Indexnummern, um das entsprechende Profil zu bearbeiten und auf die folgende Seite zu gelangen. Jedes LAN-zu-LAN-Profil beinhaltet vier Untergruppen. Ausgegraute Felder brauchen nicht ausgefüllt zu werden. Die folgenden Erläuterungen werden Ihnen dabei behilflich sein, alle notwendigen Felder auszufüllen.

Da die Web-Seite sehr umfangreich ist, sind die Erläuterungen in mehrere Abschnitte aufgeteilt.

VPN und externe Einwahl >> LAN-zu-LAN

Profil-Index : 1

1. Allgemeine Einstellungen

Profilname ???
aktiv
NetBIOS-Name durchlassen ja nein

Anrufrichtung: Beide Raus Dial-in
immer in Betrieb
Max. Leerlaufzeit 300 Sekunden
Dauer-Ping aktiv
Ping an die IP

2. Einstellungen zum Rauswählen

Verbindung zum VPN-Server über
PPTP
IPSec
L2TP mit IPSec nein

Server-IP/Hostname für VPN.
(z.B. z.B. draytek.com oder 123.45.67.89)

Benutzername ???
Passwort
PPP-Authentifizierung PAP/CHAP
VJ-Komprimierung An Aus

IKE-Authentifizierungsmethode
Pre-Shared Key
IKE Pre-Shared Key
Digitale Signatur (X.509)
nein

IPSec-Sicherheitsmethode
Mittel(AH)
Hoch(ESP) DES ohne Authentifizierung
Erweitert

Index (1-15) aus der
Verbindungstimer Konfiguration:
, , ,

Profilname	Geben Sie einen Namen für das LAN-zu-LAN-Verbindungsprofil an.
Aktiv	Dieses Kästchen markieren, um das Profil zu aktivieren.
NetBIOS-Name durchlassen	**Durchlassen** – Anklicken, damit bei der Verbindung zwischen den Hosts an beiden Enden des VPN-Tunnels der NetBIOS-Name durchgelassen wird. **Blockieren** – Falls bei der Verbindung zwischen den Hosts an beiden Enden des VPN-Tunnels ein Konflikt auftritt, kann diese Funktion die Übertragung von NetBIOS-Namen im Tunnel blockiert werden.
Anrufrichtung	Angabe der zulässigen Anrufrichtung dieses LAN-zu-LAN-Profils. **Beide** - Anwahl/Einwahl **Raus** - nur Anwahl **Rein -** nur Einwahl
Immer in Betrieb oder Max. Leerlaufzeit	**Immer in Betrieb -** Markieren Sie diesen Punkt, damit der Router die VPN-Verbindung ständig aufrecht erhält. **Max. Leerlaufzeit:** Der Standardwert beträgt 300 Sekunden. Wird die Verbindung für einen längeren Zeitraum nicht genutzt, so bricht der Router die Verbindung ab.
Dauer-Ping aktiv	Diese Funktion ermöglicht dem Router, den Status der IPSec VPN-Verbindung zu erkennen und ist besonders im Falle von anormalen Unterbrechungen des VPN IPSec-Tunnels hilfreich. Einzelheiten werden unten erläutert. Markieren Sie dieses Kästchen, um die

	Übertragung von Ping-Paketen an die angegebene IP-Adresse zu ermöglichen.
Ping an die IP	Geben Sie die IP-Adresse des entfernten Hosts an, der sich am anderen Ende des VPN-Tunnels befindet. Dauer-Ping aktiv wird für anormale Unterbrechungen von IPSec VPN-Verbindungen verwendet. Auf diese Weise kann der Status einer VPN-Verbindung ermittelt werden, aufgrund dessen der Router erkennt, ob eine Wiederwahl erforderlich ist. Wenn einer der VPN-Peers die Verbindung beenden möchte, sollten normalerweise zur gegenseitigen Information eine Reihe von Paketen ausgetauscht werden. Falls der entfernte Peer jedoch ohne vorherige Benachrichtigung abbrechen sollte, kann der Vigor-Router dies nicht wissen. Um dieses Problem zu lösen, kann der Vigor-Router ständig Ping-Pakete an den entfernten Router senden, um über den Status der VPN-Verbindung informiert zu sein und entsprechend zu reagieren. Dies geschieht unabhängig von DPD (Dead Peer Detection).
PPTP	PPTP VPN-Verbindung zum Server über das Internet aufbauen. Richten Sie für die Authentifizierung des entfernten Servers unten eine Identität mit Benutzernamen und Passwort ein.
IPSec-Tunnel	IPSec VPN-Verbindung zum Server über das Internet aufbauen.
L2TP mit …	L2TP VPN-Verbindung über das Internet aufbauen. Sie können L2TP entweder alleine oder zusammen mit IPSec wählen. Treffen Sie die Auswahl wie folgt: **Ohne:** IPSec Policy nicht anwenden. Die VPN-Verbindung über L2TP ohne IPSec kann daher als reine L2TP-Verbindung betrachtet werden. **Falls vorhanden:** Die IPSec Policy wird nur angewendet falls sie beim Verbindungsaufbau vorhanden ist. Ansonsten wird die Anwahl-VPN-Verbindung eine reine L2TP-Verbindung. **Erforderlich:** Geben Sie die IPSec Policy an, die auf jeden Fall für die L2TP-Verbindung erforderlich ist.
Benutzername	Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.
Passwort	Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.
PPP-Authentifizierung	Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen. Wegen der breiten Kompatibilität ist PAP/CHAP die üblichste Auswahl.
VJ-Komprimierung	Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen. VJ-Komprimierung wird für TCP/IP-Protokoll-Header-Komprimierung verwendet. Setzen Sie diese Option auf **Ja**, um die Bandbreite bestmöglich auszunutzen.
IKE-Authentifizierungsmethode	Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec bestimmt. **Pre-Shared Key** - Eingabe von 1-63 Zeichen als Pre-Shared Key. **Digitale Signatur (X.509)** - Wählen Sie eines der vordefinierten Profile, das unter **VPN und externe Einwahl >>IPSec-Identität** eingerichtet wurde.

IPSec-Sicherheitsmethode Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec erforderlich.

Mittel **Authentication Header (AH)** bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig aktiviert.

Hoch (ESP - Encapsulating Security Payload) - bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Treffen Sie die Auswahl wie folgt:

DES ohne Authentifizierung - DES-Verschlüsselungsalgorithmus ohne jegliche Authentifizierung verwenden.

DES mit Authentifizierung - DES-Verschlüsselungsalgorithmus mit Authentifizierungsalgorithmus MD5 oder SHA-1 verwenden.

3DES ohne Authentifizierung - 3DES-Verschlüsselungsalgorithmus ohne jegliche Authentifizierung verwenden.

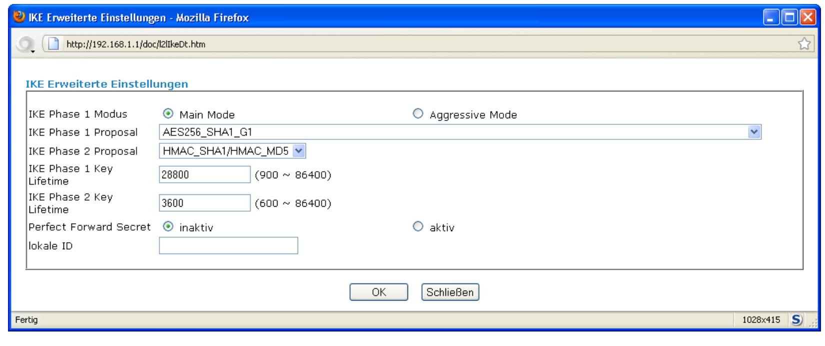
3DES mit Authentifizierung - 3DES-Verschlüsselungsalgorithmus mit Authentifizierungsalgorithmus MD5 oder SHA-1 verwenden.

AES ohne Authentifizierung - AES-Verschlüsselungsalgorithmus ohne jegliche Authentifizierung verwenden.

AES mit Authentifizierung - AES-Verschlüsselungsalgorithmus mit Authentifizierungsalgorithmus MD5 oder SHA-1 verwenden.

Erweitert Ermöglicht die Angabe von Modus, Proposal und Gültigkeitsdauer des Schlüssels jeder IKE-Phase, Gateway, usw.

Das Fenster der erweiterten Konfiguration sieht wie folgt aus:



IKE Phase 1 Modus - Sie haben die Wahl zwischen **Main** und **Aggressive**. Der Zweck besteht im Austausch von Verschlüsselungsvorschlägen zur Einrichtung eines geschützten, sicheren Kanals. Der **Main**-Modus ist sicherer als der **Aggressive**-Modus, da ein größerer Teil des Austauschs zur Einrichtung der IPSec-Sitzung über einen sicheren Kanal stattfindet. Der **Aggressive**-Modus ist jedoch schneller. Standardmäßig verwendet der Vigor-Router den Main-Modus.

IKE Phase 1 Proposal - Wird verwendet, um den VPN-Peers die lokal verfügbaren Authentifizierungsmethoden und Verschlüsselungsalgorithmen vorzuschlagen und diesbezüglich eine Rückmeldung zu erhalten. Es sind zwei Kombinationen für den **Aggressive**-Modus und neun für den **Main**-Modus verfügbar. Wir empfehlen die Auswahl der Kombination, welche die meisten Methoden abdeckt.

IKE Phase 2 Proposal - Wird verwendet, um den VPN-Peers die lokal verfügbaren Algorithmen vorzuschlagen und diesbezüglich eine Rückmeldung zu erhalten. Für beide Modi sind drei Kombinationen verfügbar. Wir empfehlen die Auswahl der

Kombination, welche die meisten Algorithmen abdeckt.

IKE Phase 1 Key Lifetime - Aus Sicherheitsgründen sollte die Gültigkeitsdauer des Schlüssels definiert werden. Der Standardwert beträgt 28800 Sekunden. Sie können einen Wert zwischen 900 und 86400 Sekunden eingeben.

IKE Phase 2 Key Lifetime - Aus Sicherheitsgründen sollte die Gültigkeitsdauer des Schlüssels definiert werden. Der Standardwert beträgt 3.600 Sekunden. Sie können einen Wert zwischen 600 und 86.400 Sekunden eingeben.

Perfect Forward Secret (PFS) - Der IKE Phase 1 Schlüssel wird wiederverwendet, um den komplexen Rechenvorgang in Phase 2 zu vermeiden. Der Standardwert dieser Funktion ist inaktiv.

Lokale ID -Im **Aggressive** Mode steht bei der Authentifizierung gegen den entfernten VPN-Server die lokale ID für die IP-Adresse. Die Länge der ID ist auf 47 Zeichen beschränkt.

3. Einstellungen zum Einwählen

Einwahl zulassen über
☑ PPTP
☑ IPSec
☑ L2TP mit IPSec [nein]

☐ Definieren Sie Remote Gateway-IP
Peer VPN-Server-IP
oder Peer-ID

Benutzername ???
Passwort
VJ-Komprimierung ◉ An ○ Aus

IKE-Authentifizierungsmethode
☑ Pre-Shared Key
IKE Pre-Shared Key
☐ Digitale Signatur (X.509)
nein

IPSec-Sicherheitsmethode
☑ Mittel(AH)
Hoch(ESP) ☑ DES ☑ 3DES ☑ AES

4. TCP/IP Netzwerk-Einstellungen

Meine WAN-IP	0.0.0.0
Remote Gateway-IP	0.0.0.0
Remote Netzwerk-IP	0.0.0.0
Remote Netzwerk-Maske	255.255.255.0

Mehr

RIP-Richtung [inaktiv]
Vom ersten bis zum entfernten Subnetz soll der VPN-Tunnel [Routen]

☐ Alle Anfragen ins Internet über diesen Tunnel leiten (nicht bei aktivem Dual-WAN möglich)

OK Löschen Abbrechen

Einwahl zulassen über Bestimmen Sie, wie die Einwahl stattfinden darf.

PPTP Dem externen Benutzer erlauben, über das Internet eine PPTP VPN-Verbindung aufzubauen. Richten Sie den Benutzernamen und das Passwort des externen Benutzers unten ein.

IPSec-Tunnel Dem externen Benutzer erlauben, über das Internet eine IPSec VPN-Verbindung anzustoßen.

L2TP Dem externen Benutzer erlauben, über das Internet eine L2TP VPN-Verbindung aufzubauen. Sie können

	L2TP entweder alleine oder zusammen mit IPSec wählen. Treffen Sie die Auswahl wie folgt: **Ohne -** IPSec Policy nicht anwenden. Die VPN-Verbindung über L2TP ohne IPSec kann daher als reine L2TP-Verbindung betrachtet werden. **Falls vorhanden** - Die IPSec Policy wird nur angewendet falls sie beim Verbindungsaufbau vorhanden ist. Ansonsten wird die Einwahl-VPN-Verbindung eine reine L2TP-Verbindung. **Erforderlich -** Geben Sie die IPSec Policy an, die auf jeden Fall für die L2TP-Verbindung erforderlich ist.
Definieren Sie das Remote VPN Gateway	Sie können die IP-Adresse des externen Benutzers oder die Peer-ID (sollte der ID entsprechen, die unter "Einwahl zulassen über" eingegeben wurde) angeben, indem Sie das Kästchen markieren. Bestimmen Sie außerdem die entsprechenden Sicherheitsmethoden auf der rechten Seite. Falls Sie das Kästchen abwählen, wendet der oben gewählte Verbindungstyp die Authentifizierungsmethoden und Sicherheitsmethoden der Basiskonfiguration an.
Benutzername	Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.
Passwort	Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.
VJ-Komprimierung	VJ-Komprimierung wird für TCP/IP-Protokoll-Header-Komprimierung verwendet. Dieses Feld wird benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen.
IKE-Authentifizierungsmethode	Diese Felder werden für IPSec-Tunnel und L2TP mit IPSec verwendet, wenn Sie die IP-Adresse des entfernten Knoten angeben. Die einzige Ausnahme ist die digitale Signatur (X.509), welche bei Auswahl des IPSec-Tunnels unter Angabe oder ohne Angabe der IP-Adresse des entfernten Knoten gesetzt werden kann. **Pre-Shared Key -** Markieren Sie das Kästchen für den Pre-Shared Key, um diese Funktion zu aktivieren, und geben Sie die erforderlichen Zeichen (1-63) als Pre-Shared Key ein. **Digitale Signatur (X.509)** – Markieren Sie das Kästchen für digitale Signatur, um diese Funktion zu aktivieren, und wählen Sie eines der vordefinierten Profile, das unter **VPN und externe Einwahl >>IPSec-Identität** eingerichtet wurde.
IPSec-Sicherheitsmethode	Diese Felder sind für IPSec-Tunnel und L2TP mit IPSec notwendig, wenn Sie den entfernten Knoten angeben. **Mittel -** Authentication Header (AH) bedeutet, dass die Daten authentifiziert, jedoch nicht verschlüsselt werden. Diese Option ist standardmäßig aktiviert. **Hoch -** Encapsulating Security Payload (ESP) bedeutet, dass die Nutzdaten sowohl verschlüsselt als auch authentifiziert werden. Als

	Verschlüsselungsalgorithmus stehen DES (Data Encryption Standard), 3DES (Triple DES) und AES zur Verfügung.
Meine WAN-IP	Dieses Feld wird nur benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen. Der Standardwert ist 0.0.0.0, was bedeutet, dass der Vigor-Router während der IPCP-Verhandlungsphase eine PPP IP-Adresse vom entfernten Router erhält. Falls die PPP IP von der entfernten Seite festgelegt wird, geben Sie hier die feste IP-Adresse ein. Ändern Sie den Standardwert nicht, falls Sie nicht PPTP oder L2TP wählen.
Remote Gateway-IP	Dieses Feld wird nur benötigt, wenn Sie oben PPTP oder L2TP mit oder ohne IPSec wählen. Der Standardwert ist 0.0.0.0, was bedeutet, dass der Vigor-Router während der IPCP-Verhandlungsphase eine entfernte Gateway PPP IP-Adresse vom entfernten Router erhält. Falls die PPP IP von der entfernten Seite festgelegt wird, geben Sie hier die feste IP-Adresse ein. Ändern Sie den Standardwert nicht, falls Sie nicht PPTP oder L2TP wählen.
Remote Netzwerk-IP/ Remote Netzwerk-Maske	Fügen Sie eine statische Route hinzu, um den gesamten Verkehr, der an diese Remote Netzwerk-IP/Remote Netzwerk-Maske gerichtet ist, durch die VPN-Verbindung zu leiten. Bei IPSec ist dies die Ziel-Client-ID von Phase 2 Quick Mode.
Mehr	Fügen Sie eine statische Route hinzu, um den gesamten Verkehr, der an weitere Remote Netzwerk-IPs/Remote Netzwerk-Masken gerichtet ist, durch die VPN-Verbindung zu leiten. Dies trifft normalerweise zu, wenn sich hinter dem entfernten VPN-Router mehrere Subnetze befinden.
RIP-Richtung	Diese Option bestimmt die Richtung der RIP-Pakete (Routing Information Protocol). Sie können hier Richtungen aktivieren/deaktivieren. Es stehen vier Optionen zur Auswahl: Beide (TX/RX), Nur TX, Nur RX und Inaktiv.
Vom ersten bis zum entfernten Subnetz soll der VPN-Tunnel	Falls das entfernte Netzwerk lediglich die Einwahl mit einer einzigen IP erlaubt, wählen Sie **NAT**, ansonsten **Route**.
Alle Anfragen ins Internet über diesen Tunnel leiten	Markieren Sie dieses Kästchen, um diesen VPN-Tunnel als Standard-Route zu bestimmen.

4.9.7 Verbindungsmanagement

Hier finden Sie eine tabellarische Zusammenfassung aller VPN-Verbindungen. Sie können jede beliebige VPN-Verbindung durch Klicken auf **Trennen** beenden. Aggressive Anwahl ist mit Hilfe des Anwahl-Tools und Klicken auf **Wählen** möglich.

VPN und externe Einwahl >> Verbindungsmanagement

Verbindung mit entferntem Netz herstellen   Aktualisierungsintervall: 10   Aktualisieren

Wählen

VPN-Verbindungsstatus

Aktuelle Seite: 1   Seite   Los   >>

VPN	Typ	Remote IP	virtuelles Netzwerk	TX-Pakete	TX-Rate(bit/s)	RX-Pakete	RX-Rate(bit/s)	Verbindung aktiv seit

xxxxxxxx : Daten sind verschlüsselt.
xxxxxxxx : Daten sind nicht verschlüsselt.

Wählen	Klicken Sie auf diese Taste, um die Anwahlfunktion auszuführen.
Aktualisierungsintervall	Wählen Sie die Zeit für die Aktualisierung der Wählinformationen: 5, 10 oder 30.
Aktualisieren	Klicken Sie auf diese Taste, um den gesamten Verbindungsstatus zu aktualisieren.

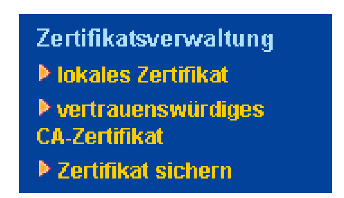
4.10 Zertifikatsverwaltung

Ein digitales Zertifikat dient als elektronischer Ausweis und wird von einer Zertifizierungsstelle (Certification Authority - CA) ausgegeben. Es enthält Informationen wie Ihren Namen, eine laufende Nummer, Verfallsdatum usw. sowie die digitale Signatur der ausgebenden Stelle, so dass ein Empfänger die Echtheit des Zertifikats verifizieren kann. Der Vigor-Router unterstützt digitale Zertifikate gemäß dem Standard X.509.

Zur Verwendung von digitalen Zertifikaten sollte zunächst ein von einem CA-Server ausgegebenes Zertifikat angefordert werden. Die Zertifikate anderer vertrauenswürdiger CA-Server sollten auch heruntergeladen werden, um die Gegenstelle mit den von diesen vertrauenswürdigen CA-Servern ausgegebenen Zertifikaten authentifizieren zu können.

Hier können Sie lokale digitale Zertifikate generieren und verwalten und vertrauenswürdige CA-Zertifikate setzen. Achten Sie darauf, dass die Uhrzeit des Vigor-Routers korrekt eingestellt ist, bevor Sie das Zertifikat verwenden, damit die Gültigkeitsdauer des Zertifikats korrekt ist.

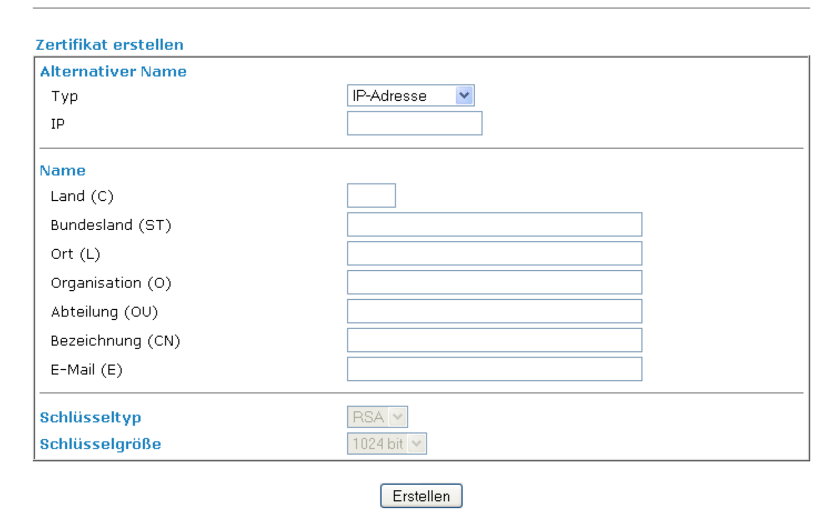
Die folgende Abbildung zeigt die Menüeinträge für das Zertifikatsverwaltung:



4.10.1 Lokales Zertifikat



Erstellen Klicken Sie auf diese Taste, um das Fenster **Zertifikat erstellen** zu öffnen.



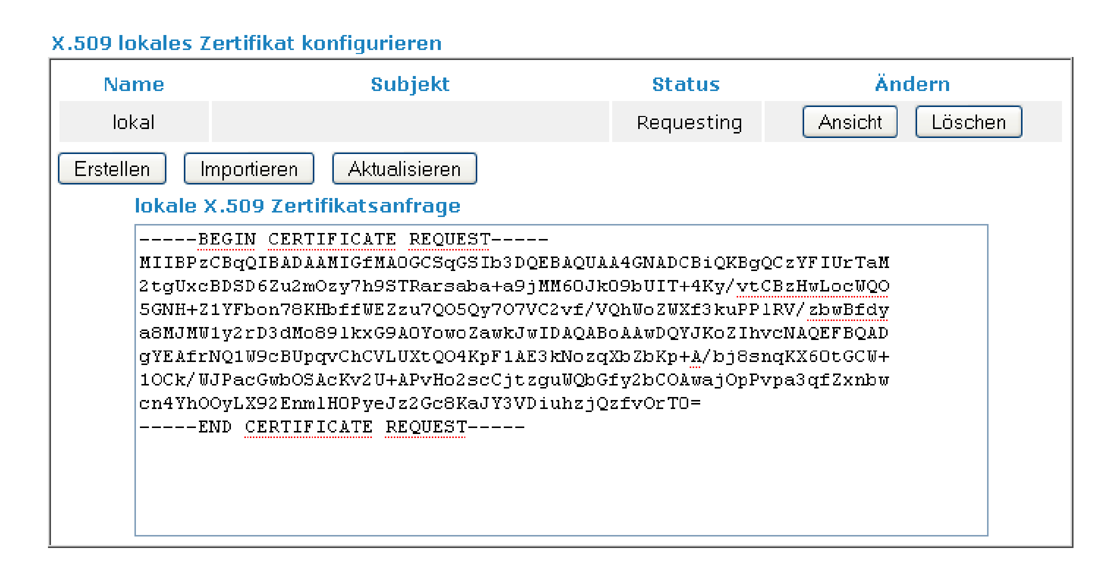
Geben Sie alle Daten ein, die das Fenster anfordert. Dann klicken Sie erneut auf **Erstellen**.

Import Klicken Sie auf diese Taste, um eine gespeicherte Datei mit Zertifizierungsinformationen zu importieren.

Aktualisieren Klicken Sie auf diese Taste, um die unten aufgeführte Information zu aktualisieren.

Ansicht Klicken Sie auf diese Taste, um die Detaileinstellungen für die Erstellung eines Zertifikats zu sehen.

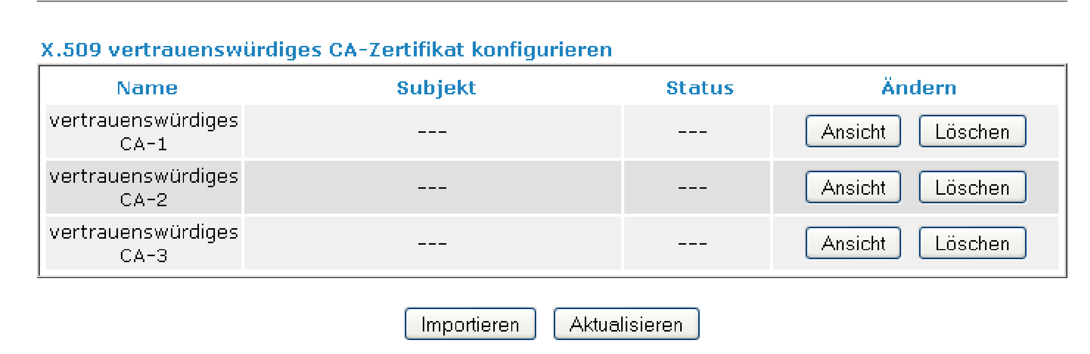
Nachdem Sie **Erstellen** angeklickt haben, wird die erzeugte Information im Fenster unten angezeigt:



4.10.2 Vertrauenswürdiges CA-Zertifikat

Unter diesem Punkt werden drei vertrauenswürdige CA-Zertifikate aufgeführt.

Zertifikatsverwaltung >> vertrauenswürdiges CA-Zertifikat



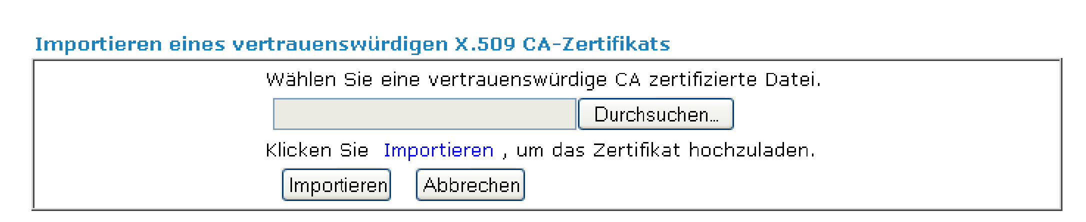
X.509 vertrauenswürdiges CA-Zertifikat konfigurieren

Name	Subjekt	Status	Ändern
vertrauenswürdiges CA-1	---	---	Ansicht Löschen
vertrauenswürdiges CA-2	---	---	Ansicht Löschen
vertrauenswürdiges CA-3	---	---	Ansicht Löschen

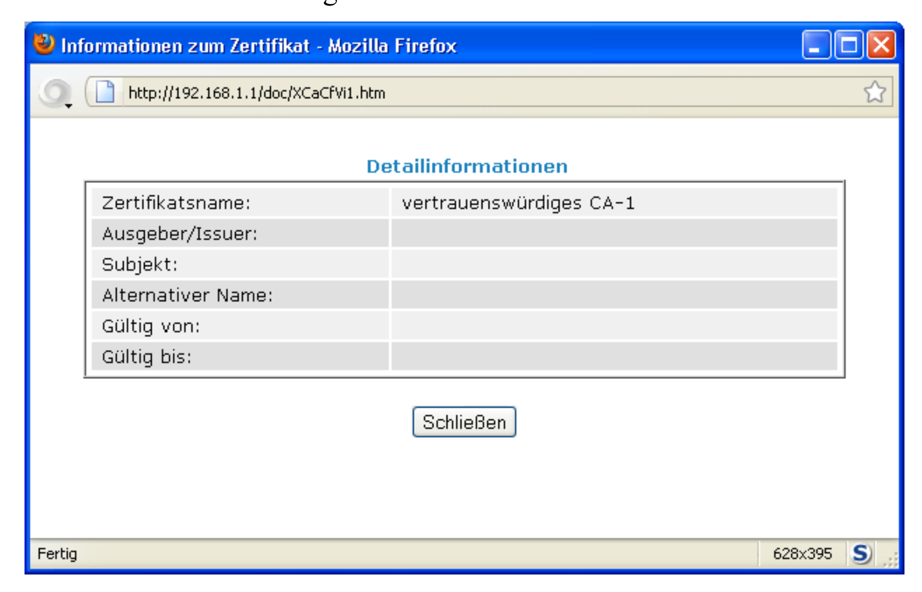
Importieren Aktualisieren

Um ein zuvor gespeichertes vertrauenswürdiges CA-Zertifikat zu importieren, klicken Sie bitte auf **Importieren**, wodurch sich das folgende Fenster öffnet. Verwenden Sie **Durchsuchen…**, um die gespeicherte Textdatei zu finden. Dann klicken Sie auf **Importieren**. Das importierte Zertifikat wird im Fenster für vertrauenswürdige CA-Zertifikate aufgeführt.

Zertifikatsverwaltung >> vertrauenswürdiges CA-Zertifikat



Sie können die einzelnen vertrauenswürdigen CA-Zertifikate betrachten, indem Sie das detaillierte Infofenster durch Klicken auf **Ansicht** öffnen. Um ein CA-Zertifikat zu löschen, markieren Sie es und klicken auf **Löschen**, wodurch alle Zertifikatsinformationen gelöscht werden.



4.10.3 Zertifikat sichern

Das lokale Zertifikat und das vertrauenswürdige CA-Zertifikat für diesen Router können in einer Datei gespeichert werden. Klicken Sie im folgenden Dialog auf **Backup**, um die Zertifikate zu speichern. Falls Sie ein Verschlüsselungspasswort für diese Zertifikate setzen möchten, geben Sie bitte die entsprechenden Zeichenfolgen in **Verschlüsselungspasswort** und **Passwort bestätigen** ein.

Sie können jederzeit **Wiederherstellen** verwenden, um diese beiden Einstellungen auf dem Router wiederherzustellen.

Zertifikatsverwaltung >> Zertifikat sichern

Erstellen / Laden eines Zertifikats

Datensicherung

Verschlüsselungspasswort:

Passwort bestätigen:

Klicken Sie [Datensicherung] , um Zertifikate als Backup-Datei auf Ihrem Computer zu speichern.

Wiederherstellen

Wählen Sie eine Backup-Datei aus.

[Durchsuchen...]

Entschlüsselungspasswort:

Klicken Sie [Wiederherstellen] , um die Datei hochzuladen.

4.11 Wireless LAN

Diese Funktion wird nur für das "n"-Modell verwendet.

4.11.1 Grundlagen

In den letzten Jahren ist der Markt für kabellose Kommunikation enorm gewachsen. Praktisch jeder Punkt auf der Erde wird mit Wireless-Technologie erreicht oder kann erreicht werden. Viele Menschen tauschen jeden Tag über Wireless-Kommunikationsprodukte Informationen aus. Das Vigor-Modell "n", d.h. der Vigor-Wireless-Router, wurde im Hinblick auf maximale Flexibilität und Effizienz im Kleinunternehmen/Privatbereich konzipiert. Jeder berechtigte Mitarbeiter kann ohne Kabelsalat und Löcher in den Wänden ein WLAN-fähiges PDA oder Notebook im Besprechungszimmer verwenden. Die Mobilität im Wireless LAN ist so hoch entwickelt, dass WLAN-Benutzer gleichzeitig Zugriff auf die gesamte LAN-Ausstattung und auf das Internet haben, genau wie dies bei einem kabelgebundenen LAN der Fall wäre.

Vigor-Wireless-Router sind mit einer WLAN-Schnittstelle ausgerüstet, die dem Standard IEEE 802.11n entspricht. Die fortgeschrittene Wireless-Technologie des Vigor-Routers sorgt für eine weitere Leistungssteigerung, die Übertragungsgeschwindigkeiten von bis zu 300 Mbps* ermöglicht. Endlich können Sie nun ruckelfreie Audio- und Videoübertragungen genießen!

Hinweis: * Der tatsächliche Datendurchsatz ändert sich je nach Netzwerkbedingungen und Faktoren wie dem Netzwerkverkehrsvolumen, dem Netzwerk-Overhead und den Objekten in der Umgebung.

In einem Wireless-Netzwerkinfrastrukturmodus dient der Vigor-Wireless-Router als Access Point (AP), mit dem sich verschiedene WLAN-Clients bzw. Stationen (STA) verbinden können. Alle STAs teilen sich den gleichen Internetanschluss über den Wireless-Router. Unter **Basiskonfiguration** werden die Daten zu diesem Wireless-Netzwerk wie die SSID, der Kanal usw. eingestellt.

Verschlüsselungsfunktionen

Echtzeit-Hardware-Verschlüsselung: Der Vigor-Router ist mit einer Hardware-AES-Verschlüsselungs-Engine ausgestattet, um maximalen Schutz der Daten ohne Beeinträchtigung der Nutzung zu ermöglichen.

Umfassende Auswahl von Verschlüsselungsnormen: Um die Sicherheit und die Vertraulichkeit Ihrer Wireless-Kommunikation zu sichern, bieten wir verschiedene marktübliche Normen an.

WEP (Wired Equivalent Privacy) ist eine ältere Methode zur Verschlüsselung jedes per Funk übertragenen Datenpakets mit einem 64- oder 128-Bit-Schlüssel. Normalerweise gibt der Access Point vier Schlüssel vor, wobei nur einer für die Kommunikation mit den einzelnen Clients verwendet wird.

WPA (Wi-Fi Protected Access), der vorherrschende Sicherheitsmechanismus in diesem Sektor, umfasst zwei Kategorien: WPA-Personal, auch bekannt als WPA Pre-Shared Key (WPA/PSK), und WPA-Enterprise, auch bekannt als WPA/802.1x.

Bei WPA-Personal wird während der Datenübertragung ein Pre-Shared Key (vorher vereinbarter Schlüssel) für die Verschlüsselung verwendet. WPA benutzt für die Datenverschlüsselung Temporal Key Integrity Protocol (TKIP), und WPA2 verwendet AES. WPA-Enterprise wird nicht nur für die Verschlüsselung, sondern auch für die Authentifizierung benutzt.

Da sich herausgestellt hat, dass WEP verletzlich ist, ist WPA als sicherste Verbindung zu empfehlen. Wählen Sie Ihren Bedürfnissen entsprechend den geeignetsten Sicherheitsmechanismus. Letztendlich verbessert jede Sicherheitsfunktion den Schutz Ihrer Funkdaten und/oder die Privatsphäre Ihres Wireless-Netzwerks. Der Wireless-Router von Vigor ist sehr flexibel und unterstützt gleichzeitig mehrere sichere Verbindungen mit WEP und WPA.

Die **Trennung des Wireless LAN vom kabelgebundenen LAN (WLAN-Isolation)** ermöglicht Ihnen, Ihr Wireless LAN für Quarantäne- oder Zugriffsbeschränkungszwecke vom kabelgebundenen LAN zu isolieren. "Isolieren" bedeutet in diesem Zusammenhang, dass die Parteien keinen Zugriff aufeinander haben. Im geschäftlichen Bereich kann beispielsweise ein Wireless LAN speziell für Besucher eingerichtet werden, so dass diese Zugang zum Internet haben, ohne jedoch auf vertrauliche Daten zugreifen zu können. Weitere Flexibilität kann dadurch erreicht werden, dass MAC-Adressfilter eingesetzt werden, um den Zugriff von Benutzern des kabelgebundenen LANs zu isolieren.

Die **Verwaltung der Wireless-Clients (Liste der Clients)** führt alle Clients in Ihrem Wireless-Netzwerk und ihren Verbindungsstatus auf. Die folgende Abbildung zeigt die Menüeinträge für Wireless LAN an:

Wireless LAN
- Basiskonfiguration
- Verschlüsselung
- Zugriffskontrolle
- WPS
- WDS
- phy. WLAN-Modi
- WMM
- Liste der Access-Points
- Liste der Clients

4.11.2 Basiskonfiguration

Wenn Sie auf **Basiskonfiguration** klicken, erscheint eine neue Web-Seite, auf der Sie die SSID und den Wireless-Kanal einstellen können. Die folgende Abbildung enthält weitere Informationen:

Wireless LAN >> Basiskonfiguration

Basiskonfiguration (IEEE 802.11)

☑ aktiv

Modus: gemischt (11b+11g+11n)

Index (1-15) aus der Verbindungstimer Konfiguration: , , ,

Es werden nur die Verbindungstimer-Profile berücksichtigt, in denen die Aktion <Verbindung beenden> ausgewählt wurde.

	Aktiv	SSID verbergen	SSID	Isolierung von LAN	Mitglieder
1		☐	DrayTek	☐	☐
2	☐	☐		☐	☐
3	☐	☐		☐	☐
4	☐	☐		☐	☐

SSID verbergen: Nach der SSID kann nicht gescannt werden, da sie nach außen hin nicht angezeigt wird.

Mitglieder isolieren: WLAN-Clients einer SSID können nicht untereinander kommunizieren.

LAN isolieren: WLAN-Clients einer SSID können nicht mit den kabelgebundenen LAN-PC's kommunizieren.

Kanal: Kanal 6, 2437MHz Long Preamble: ☐

Long Preamble: Nur bei Problemen mit alten 802.11b Karten verwenden (Performanz-Einbußen).

Packet-OVERDRIVE™

☐ TX-Burst

Hinweis:

Damit die WLAN-Performance verstärkt wird, muss die selbe Technologie auch von dem drahtlos Client unterstützt werden.

Bandbreite

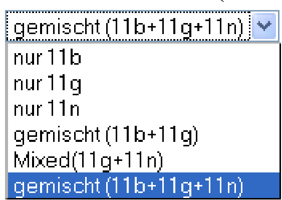
	Aktiv	Upload		Download	
SSID 1	☐	30000	kbit/s	30000	kbit/s
SSID 2	☐	30000	kbit/s	30000	kbit/s
SSID 3	☐	30000	kbit/s	30000	kbit/s
SSID 4	☐	30000	kbit/s	30000	kbit/s

Hinweis: Der gültige Wertebereich liegt zwischen 100~50.000 kbit/s

OK Abbrechen

Aktiv Markieren Sie dieses Kästchen, um die Wireless-Funktion zu aktivieren.

Modus Zur Zeit kann sich der Router über die Modi Gemischt (11b+11g), Nur 11g, Nur 11b, Gemischt (11g+11n), Nur 11n und Gemischt (11b+11g+11n) mit Clients verbinden. Wählen Sie einfach den Modus Gemischt (11b+11g+11n).



Hinweis: Bei Auswahl der Modi Nur 11g, Nur 11b oder Nur 11n sollten Sie gleichzeitig den **RADIUS-Server** aktivieren.

Index (1-15)
Sie können das Wireless LAN so konfigurieren, dass es lediglich in gewissen Zeitabschnitten in Betrieb ist. Sie können bis zu vier der 15 vordefinierten Timer unter **Anwendungen** >> **Timer** wählen. Per Standardeinstellung ist dieses Feld leer, und die Funktion ist ständig in Betrieb.

SSID verbergen
Markieren Sie dieses Kästchen, um Wireless-Sniffing zu vermeiden und es für unbefugte Clients oder STAs schwieriger zu machen, sich an Ihrem Wireless LAN anzumelden. Je nach verwendeter Wireless-Technik kann der Benutzer bei der Netzwerksuche lediglich die Information ohne SSID oder überhaupt nichts über den Vigor-Wireless-Router sehen. Das System erlaubt die Eingabe von vier verschiedenen SSIDs für unterschiedliche Zwecke. Standardmäßig wird die erste SSID aktiviert. Sie können diese bei Bedarf verbergen.

SSID
Dies ist die Bezeichnung des Wireless LANs. Die SSID kann aus alphanumerischen Zeichen und Sonderzeichen bestehen. Die Standard-SSID ist "DrayTek". Wir empfehlen, diese zu ändern.

Isolierung von
LAN – Markieren Sie dieses Kästchen, damit Wireless-Clients mit der gleichen SSID keinen Zugriff auf kabelgebundene PCs im LAN haben.

Mitglied – Markieren Sie dieses Kästchen, damit Wireless-Clients mit der gleichen SSID keinen gegenseitigen Zugriff haben.

Kanal
Gibt den Frequenzkanal des Wireless LANs an. Der Standardkanal ist 6. Ändern Sie den gewählten Kanal, falls dieser starken Funkstörungen ausgesetzt ist. Falls Sie nicht wissen, welche Frequenz geeignet ist, wählen Sie Auto, um das System die Auswahl treffen zu lassen.

automatisch
automatisch
Kanal 1, 2412MHz
Kanal 2, 2417MHz
Kanal 3, 2422MHz
Kanal 4, 2427MHz
Kanal 5, 2432MHz
Kanal 6, 2437MHz
Kanal 7, 2442MHz
Kanal 8, 2447MHz
Kanal 9, 2452MHz
Kanal 10, 2457MHz
Kanal 11, 2462MHz
Kanal 12, 2467MHz
Kanal 13, 2472MHz

Long Preamble
Diese Option dient der Bestimmung der Länge des Sync-Feldes in einem 802.11-Paket. Die meisten modernen Wireless-Netzwerke verwenden kurze Präambeln mit 56-Bit Sync-Feld anstatt der langen Präambel mit 128-Bit Sync-Feld. Manche originäre 11b Wireless-Netzwerkgeräte unterstützen jedoch nur lange Präambeln. Markieren Sie **Long Preamble**, falls dies erforderlich ist, um mit dieser Art von Geräten zu kommunizieren.

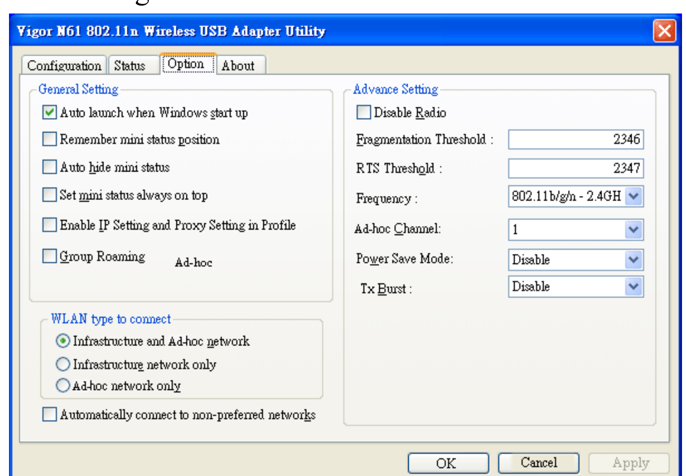
Packet-OVERDRIVE

Diese Funktion kann die Datenübertragungsleistung um ca. 40%* verbessern (durch Markieren von **Tx-Burst**). Es ist aktiv, wenn sowohl der Access Point als auch die Station (im Wireless-Client) die Funktion gleichzeitig verwendet. Dies bedeutet, dass der Wireless-Client diese Funktion sowohl unterstützen als auch aktivieren muss.

Hinweis: Der Vigor N61 Wireless Adapter unterstützt diese Funktion. Sie können diesen verwenden und in Ihrem Rechner installieren, um die Nutzung von Packet-OVERDRIVE zu ermöglichen (sehen Sie das folgende Bild des Vigor N61 Wireless Konfigurationsfensters; hier muss im Fenster **Optionen** die Funktion **TxBURST** auf **Aktiv** gesetzt werden).

Bandbreite

Legt die Datenübertragungsgeschwindigkeit über die kabellose Verbindung fest.



Upload – Klicken Sie auf **Aktiv** und geben Sie die Übertragungsgeschwindigkeit für Uploads an. Der Standardwert beträgt 30.000 kbps.

Download – Geben Sie die Übertragungsgeschwindigkeit für Downloads an. Der Standardwert beträgt 30.000 kbps.

4.11.3 Verschlüsselung

Diese Seite ermöglicht Ihnen die Konfiguration der Sicherheit mit verschiedenen Modi für SSID 1, 2, 3 und 4. Nach Abschluss der Konfiguration klicken Sie bitte auf **OK**, um die Einstellungen zu speichern und anzuwenden.

Wenn Sie auf **Verschlüsselung** klicken, erscheint eine neue Web-Seite, auf der Sie die WEP- und WPA-Einstellungen konfigurieren können.

Wireless LAN >> Sicherheitseinstellungen

SSID 1 | SSID 2 | SSID 3 | SSID 4

Verschlüsselung: WPA2/PSK

WPA:

Variante: TKIP

Pre-Shared Key(PSK): ************

Geben Sie 8~63 ASCII-Zeichen oder 64 hexadezimale Zahlen beginnend mit "0x", z.B.: "cfgs01a2..." or "0x655abcd....".

WEP:

Variante: 64-bit

Schlüssel 1 : *************

Schlüssel 2 : *************

Schlüssel 3 : *************

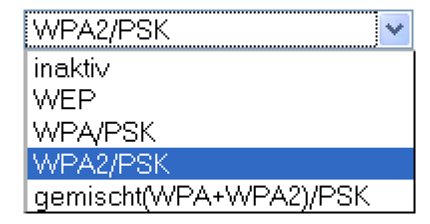
Schlüssel 4 : *************

für 64 bit WEP-Schlüssel
Geben Sie 5 ASCII-Zeichen oder 10 hexadezimale Zahlen beginnend mit "0x", z.B.: "AB312" oder "0x4142333132".

für 128 bit WEP-Schlüssel
Geben Sie 13 ASCII-Zeichen oder 64 hexadezimale Zahlen beginnend mit "0x", z.B.: "0123456789abc" oder "0x30313233343536373839414243".

OK | Abbrechen

Modus Es stehen verschiedene Modi zur Auswahl.



Inaktiv - Verschlüsselung abschalten.

WEP - Akzeptiert nur WEP-Clients; der Schlüssel für die Verschlüsselung muss unter WEP-Schlüssel eingetragen werden.

WPA/PSK - Akzeptiert nur WPA-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingeben werden.

WPA2/PSK -Akzeptiert nur WPA2-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingegeben werden.

Gemischt (WPA+ WPA2)/PSK - Akzeptiert gleichzeitig WPA- und WPA2-Clients; der Schlüssel für die Verschlüsselung muss unter PSK eingegeben werden.

WPA	WPA verschlüsselt jedes per Funk übertragene Paket entweder mit dem PSK (Pre-Shared Key), der in dem Feld unten manuell eingegeben wurde, oder mit dem automatisch per 802.1x-Authentifizierung verhandelten Schlüssel. Hierzu werden entweder **8~63** ASCII-Zeichen, z.B. "012345678..." oder 64 hexadezimale Ziffern, angeführt von "0x", z.B. "0x321253abcde..." verwendet. **Typ** - Auswahl zwischen Gemischt (WPA+WPA2) oder Nur WPA2. **Pre-Shared Key (PSK)** - Entweder **8~63** ASCII-Zeichen, z.B. "012345678..." oder 64 hexadezimale Zeichen, angeführt von "0x", z.B. "0x321253abcde...".
WEP	**64-Bit** - Für 64-Bit WEP-Schlüssel; entweder **5** ASCII-Zeichen, z.B. "12345", oder 10 hexadezimale Ziffern, angeführt von "0x", z.B. "0x4142434445". **128-Bit** - Für 128-Bit WEP-Schlüssel; entweder **13** ASCII-Zeichen, z.B. "ABCDEFGHIJKLM", oder 26 hexadezimale Ziffern, angeführt von "0x", z.B. "0x4142434445464748494A4B4C4D".  Alle Wireless-Geräte müssen die gleiche WEP-Verschlüsselungslänge unterstützen und den gleichen Schlüssel verwenden. Hier können **vier Schlüssel** eingegeben werden, aber es kann jeweils nur ein Schlüssel ausgewählt werden. Die Schlüssel können in ASCII oder hexadezimal eingegeben werden. Haken Sie den Schlüssel an, den Sie verwenden möchten.

4.11.4 Zugriffskontrolle

Um den Wireless-Zugriff zusätzlich abzusichern, ermöglicht Ihnen die **Zugriffskontrolle**, den Zugriff auf das Netzwerk über die Wireless LAN MAC-Adresse des Clients zu steuern. So wird nur gültigen MAC-Adressen erlaubt, auf die Wireless LAN Schnittstelle zuzugreifen. Wenn Sie auf **Zugriffskontrolle** klicken, erscheint eine neue Web-Seite wie unten abgebildet, in der Sie die MAC-Adressen der Clients bearbeiten können, um deren Zugriffsrechte zu steuern.

Wireless LAN >> Zugriffskontrolle

Zugriffskontrolle

MAC-Adressen Filter aktivieren

☐ SSID 1 ☐ SSID 2 ☐ SSID 3 ☐ SSID 4

MAC-Adressen Filter

Index Attribut MAC-Adresse

Client MAC-Adresse : : : : : :

Attribut :

☐ s: Client vom LAN isolieren

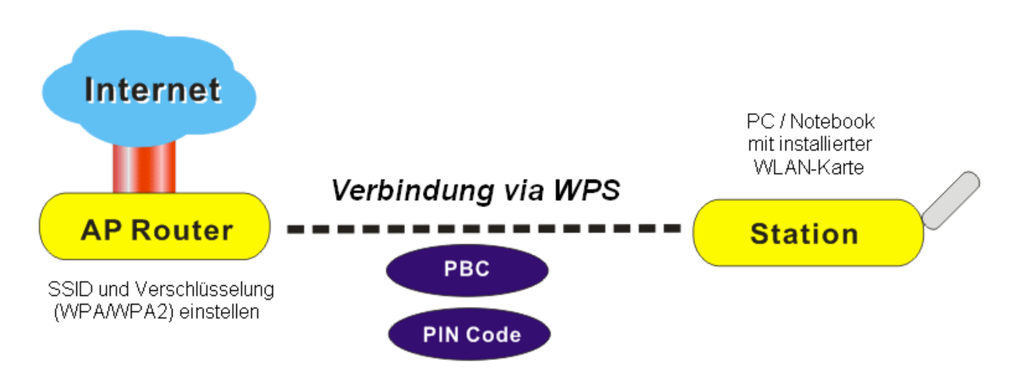
Hinzufügen Löschen Bearbeiten Abbrechen

OK Alles löschen

MAC-Whitelist	Hier kann der MAC-Adressenfilter für das Wireless LAN für SSID 1 bis 4 aktiviert werden. Alle im Feld aufgeführten Clients (ausgedrückt durch MAC-Adressen) können in verschiedene Wireless LANs gruppiert werden. Falls Sie beispielsweise SSID 1 und SSID 2 markieren, können sie gleichzeitig unter SSID 1 und SSID 2 gruppiert werden.
MAC-Adressenfilter	Alle MAC-Adressen anzeigen, die zuvor bearbeitet wurden.
MAC-Adresse des Clients	Geben Sie die MAC-Adresse des Wireless-Clients manuell ein.
Attribut	**s: Client vom LAN isolieren -** Markieren, um die Wireless-Verbindung des Wireless-Clients mit der MAC-Adresse vom LAN zu trennen.
Hinzufügen	Der Liste eine neue MAC-Adresse hinzufügen.
Löschen	Ausgewählte MAC-Adresse aus der Liste löschen.
Bearbeiten	Ausgewählte MAC-Adresse in der Liste bearbeiten.
Abbrechen	Konfiguration der Zugriffskontrolle abbrechen.
OK	ACL speichern.
Alle löschen	Alle Einträge in der MAC-Adressenliste löschen.

4.11.5 WPS

WPS (Wi-Fi Protected Setup) ist eine einfache Methode, um WPA- und WPA2-verschlüsselte Netzwerkverbindungen zwischen WLAN-Clients und dem Wireless Access Point (Vigor-Router) aufzubauen.

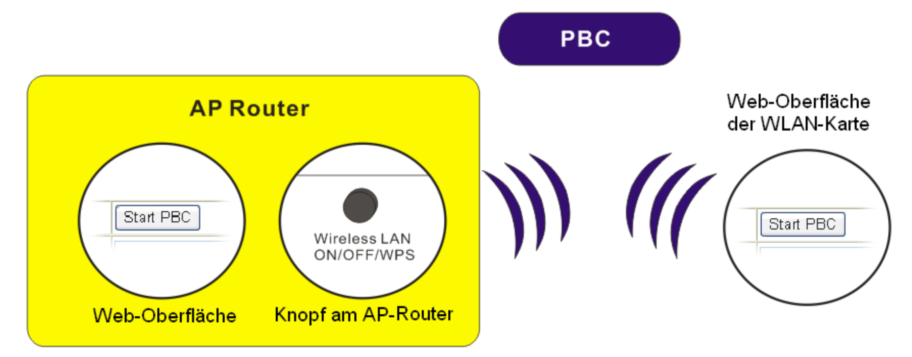


Hinweis: Diese Funktion ist nur für WLAN-Clients verfügbar, die WPS unterstützen.

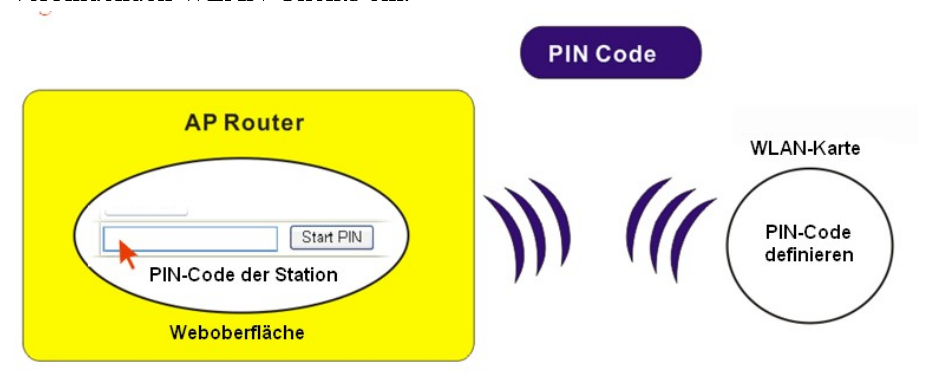
Dies ist der einfachste Ansatz zum Aufbau einer Verbindung zwischen WLAN-Clients und dem Vigor-Router. Benutzer brauchen nicht jedes Mal den Verschlüsselungsmodus zu wählen und ein langes Verschlüsselungspasswort einzugeben, um einen WLAN-Client einzurichten. Es ist ausreichend, auf dem WLAN-Client auf eine Taste zu drücken, um den Client automatisch über WPS mit dem Router zu verbinden.

Die Netzwerkverbindung über WPS zwischen dem AP und den Clients kann in zweierlei Weise aufgebaut werden: Durch Drücken auf ***Starte PBC*** oder durch Eingabe des ***PIN-Codes***.

- Drücken Sie auf dem als AP konfigurierten Vigor 2710 Router auf die **WPS**-Taste an der Vorderseite des Routers oder klicken Sie im Web-Konfigurationsmenü auf **Starte PBC**. Auf dem Client, auf dem die Netzwerkkarte installiert ist, drücken Sie auf **Starte PBC** der Netzwerkkarte.



- Um den PIN-Code zu benutzen, müssen Sie den im WLAN-Client angegebenen PIN-Code kennen. Geben Sie den PIN-Code des mit dem Vigor-Router zu verbindenden WLAN-Clients ein.



- Da WPS entweder WPA-PSK oder WPA2-PSK erfordert, wird die folgende Meldung angezeigt, falls Sie nicht in Wireless LAN>>Verschlüsselung einen dieser Modi wählen.



Klicken Sie auf **OK** und gehen Sie zurück zu **Wireless LAN>>Verschlüsselung**, um WPA-PSK oder WPA2-PSK zu wählen, und starten Sie WPS erneut.

Web-Seite für **Wireless LAN>>WPS**:

Wireless LAN >> WPS (Wi-Fi Protected Setup)

☑ aktiv

WPS-Information

WPS-Status	Konfiguriert
SSID	DrayTek
Authentifizierungs-Modus	inaktiv

Gerätekonfiguration

Konfiguration per Knopfdruck (PBC)	Starte PBC
Konfiguration via PIN-Code	Start-PIN

Status: Die Authentifizierung geschieht nicht über WPA/WPA2 PSK!

Hinweis: WPS erleichtert die WLAN-Sicherheitskonfiguration durch automatisches Hinzufügen der wireless Clients zum Access Point.
: WPS ist inaktiv.
: WPS ist aktiv.
: Warte auf WPS-Anfragen von wireless Clients.

Aktiv	Markieren Sie dieses Kästchen, um WPS zu aktivieren.

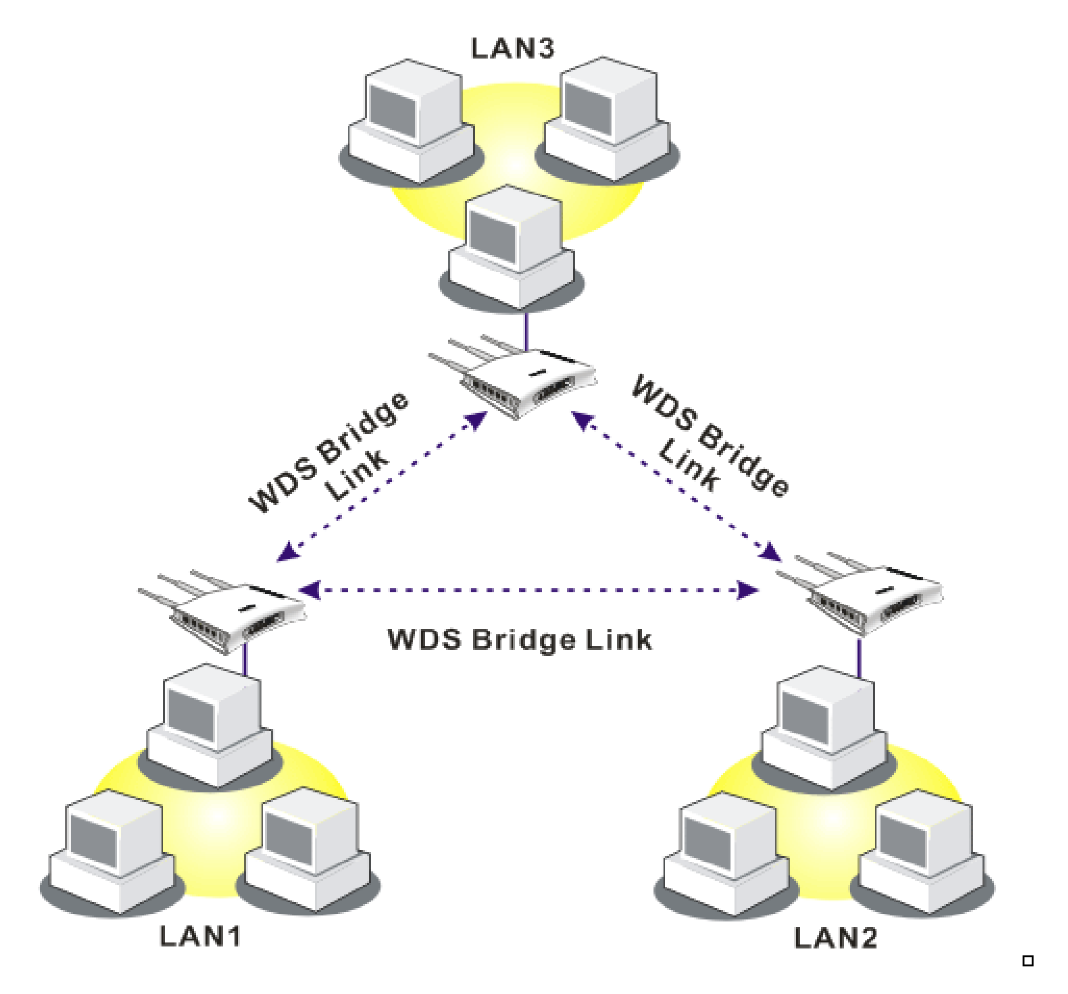
WPS-Status	Zeigt WPS-bezogene Systeminformationen an. Wenn die Wireless-Sicherheit (Verschlüsselung) des Routers richtig konfiguriert ist, erscheint hier die Meldung "Konfiguriert".
SSID	SSID1 des Routers anzeigen. WPS wird nur von SSID1 unterstützt.
Authentifizierungs-Modus	Aktuellen Authentifizierungs-Modus des Routers anzeigen. Nur WPA2/PSK und WPA/PSK unterstützen WPS.
Konfiguration per Knopfdruck (PBC)	Klicken Sie auf **Starte PBC**, um die WPS-Einrichtung per Knopfdruck zu starten. Der Router wartet ca. zwei Minuten auf WPS-Anfragen von WLAN-Clients. Während WPS in Betrieb ist, blinkt die WPS-LED am Router schnell. Die LED kehrt nach zwei Minuten in den Normalzustand zurück (d.h. WPS muss innerhalb von zwei Minuten eingerichtet werden).
Konfiguration via PIN-Code	Geben Sie den PIN-Code des zu verbindenden WLAN-Clients ein und klicken Sie auf **Start-PIN**. Während WPS in Betrieb ist, blinkt die WPS-LED am Router schnell. Die LED kehrt nach zwei Minuten in den Normalzustand zurück (d.h. WPS muss innerhalb von zwei Minuten eingerichtet werden).

4.11.6 WDS

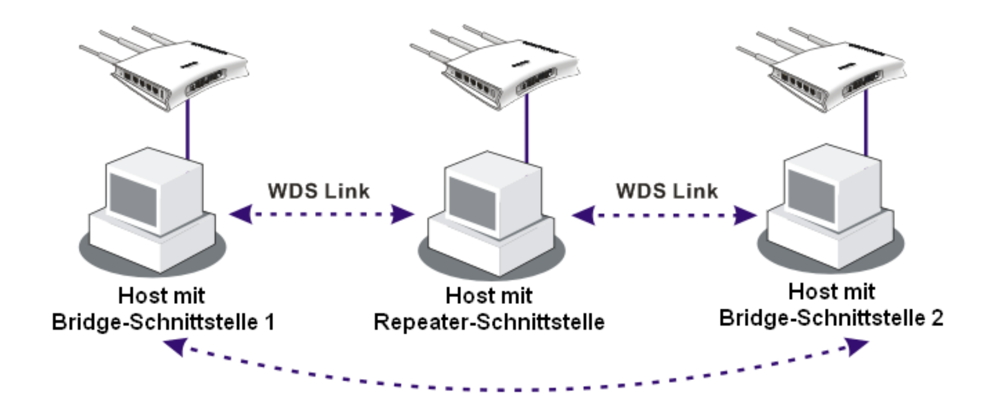
WDS ist die Abkürzung für Wireless Distribution System. Es handelt sich hierbei um ein Protokoll zur drahtlosen Verbindung von zwei Access Points (AP). Üblicherweise wird diese Technik für die folgenden Zwecke eingesetzt:

- Drahtlose Überbrückung zweier LANs.
- Erweiterte Reichweite eines WLANs.

Um diese Anforderungen zu erfüllen, bietet der Vigor-Router zwei WDS-Modi: **Bridge** und **Repeater**. Die folgende Abbildung zeigt die Funktionsweise der WDS-Bridge-Schnittstelle:

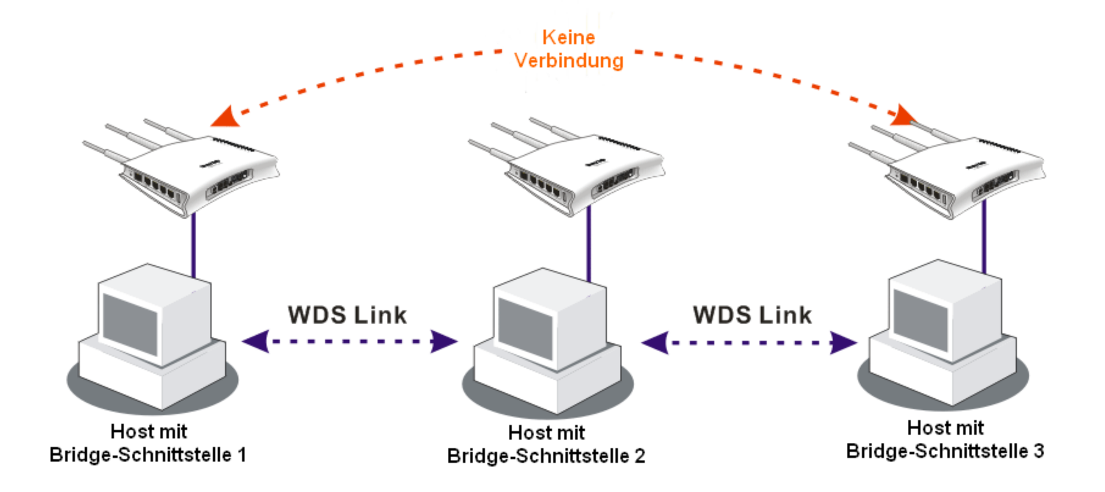


Die WDS-Repeater-Anwendung funktioniert wie folgt:



Der Hauptunterschied zwischen diesen beiden Modi ist wie folgt: Im **Repeater**-Modus werden die von einem Peer-AP empfangenen Pakete über WDS-Verbindungen an andere Peer-APs wiederholt. Im **Bridge**-Modus hingegen werden Pakete, die über eine WDS-Verbindung empfangen wurden, lediglich an lokale kabelgebundene oder Wireless-Hosts weitergeleitet. Anders ausgedrückt ist nur der Repeater-Modus in der Lage, Pakete von WDS zu WDS zu übertragen.

In den folgenden Beispielen können mit Bridge 1 oder 3 verbundene Hosts über WDS-Verbindungen mit Hosts kommunizieren, die mit Bridge 2 verbunden sind. Hosts, die mit Bridge 1 verbunden sind, können jedoch NICHT mit Hosts kommunizieren, die über Bridge 2 mit Bridge 3 verbunden sind.



Klicken Sie im Menü **Wireless LAN** auf **WDS**. Die folgende Seite erscheint:

Wireless LAN >> Wireless Distributed System

Wireless Distributed System | Auf Werkseinstellungen zurücksetzen |

Modus: Bridge

Sicherheit:
inaktiv WEP WPA

WEP:
Den selben WEP-Schlüssel verwenden wie unter Verschlüsselung.

WPA:
Typ : TKIP
Schlüssel (Key) : ************

Geben Sie 8~63 ASCII-Zeichen oder 64 hexadezimale Zahlen beginnend mit "0x" ein; z.B.: "cfgs01a2..." oder "0x655abcd....".

Bridge
Aktiv MAC-Adresse

Hinweis: Für eine bessere Performanz sollten unbenutzte Verbindungen deaktiviert werden.

Repeater
Aktiv MAC-Adresse

Access-Point Funktion:
aktiv inaktiv

Status:
Sende ein "Hallo" zu den anderen Stationen.

Verbindungsstatus

Hinweis: Diese Funktion ist nur zulässig, wenn die Station diese ebenfalls unterstützt.

OK Abbrechen

Modus	Wählen Sie den Modus für die WDS-Einstellungen. **Inaktiv** bedeutet, dass keine WDS-Einstellungen verwendet werden. Der **Bridge**-Modus dient dem ersten Anwendungsfall. Der **Repeater**-Modus dient dem zweiten Anwendungsfall. Bridge inaktiv Bridge Repeater
Verschlüsselung	Es stehen drei Optionen zur Auswahl: **Inaktiv**, **WEP** und **Pre-Shared Key**. Die hier gewählte Einstellung bestimmt, ob das folgende WEP oder Pre-Shared Key Feld zutrifft oder nicht. Wählen Sie einen der Typen für den Router.
WEP	Markieren Sie dieses Kästchen, um den gleichen Schlüssel zu verwenden, der auf der Seite **Verschlüsselung** gesetzt wurde. Falls auf der Seite **Verschlüsselung** kein Schlüssel gesetzt wurde, ist dieses Kästchen inaktiv.
Pre-Shared Key	Geben Sie 8 ~ 63 ASCII-Zeichen 64 hexadezimale Ziffern, angeführt von "0x", ein.
Bridge	Falls Sie als Verbindungsmodus **Bridge** wählen, geben Sie bitte die MAC-Adresse der Peers in diesen Feldern ein. Es können bis zu vier MAC-Adressen von Peers gleichzeitig eingegeben werden. Bitte deaktivieren Sie jedoch unbenutzte Verbindungen, um die Leistung zu verbessern. Markieren Sie nach der Eingabe das Kästchen **Aktiv** vor der MAC-Adresse, um die entsprechende MAC-Adresse zu aktivieren.
Repeater	Falls Sie als Verbindungsmodus **Repeater** wählen, geben Sie bitte die MAC-Adresse der Peers in diesen Feldern ein. Es können bis zu vier MAC-Adressen von Peers gleichzeitig eingegeben werden. Markieren Sie nach der Eingabe das Kästchen **Aktiv** vor der MAC-Adresse, um die entsprechende MAC-Adresse zu aktivieren.
Access-Point Funktion	Klicken Sie auf **Aktiv**, um diesen Router als Access Point zu verwenden; klicken Sie auf **Inaktiv**, um diese Funktion auszuschalten.
Status	Hiermit können den Peers "hello"-Meldungen geschickt werden, vorausgesetzt, die Peers unterstützen diese Funktion.

4.11.7 Liste der Access Points

Vigor-Router können alle Standardkanäle scannen und in Betrieb befindliche APs in der Umgebung auffinden. Aufgrund des Suchergebnisses erfahren Benutzer, welcher Kanal zur Benutzung geeignet ist. Diese Funktion kann auch zur Suche nach einem AP für eine WDS-Verbindung genutzt werden. Beachten Sie, dass sich kein Client während des Suchprozesses (ca. 5 Sekunden) mit dem Vigor-Router verbinden kann.

Diese Seite wird zur Suche von APs im Wireless LAN verwendet. Es werden jedoch nur APs erkannt, die sich auf dem gleichen Kanal befinden, wie dieser Router. Klicken Sie auf **Suchen**, um alle verbundenen APs zu erkennen.

Wireless LAN >> Liste der Access-Points

Liste der Access-Points

BSSID Kanal SSID

Suchen

Zur AP-Statistik.

Hinweis: Während dem Scanvorgang (~5 Sekunden) darf sich keine Station mit dem Router verbinden.

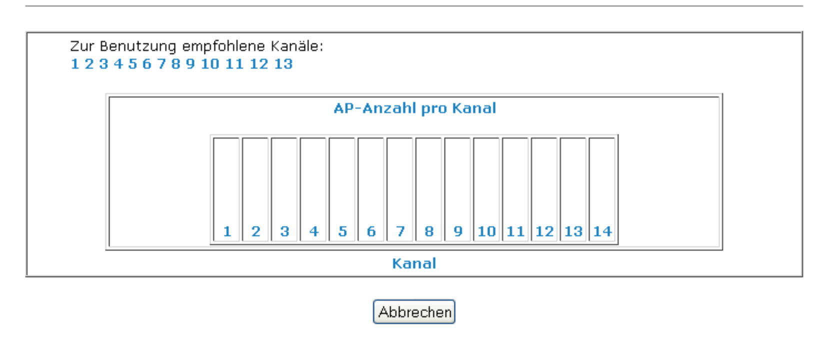
Hinzufügen zu WDS :

APs MAC-Adresse : : : : :

Hinzufügen zu ◉ Bridge ○ Repeater

Suchen Sucht nach allen verbundenen APs. Die Ergebnisse werden im Feld über dieser Taste angezeigt.

Statistik Zeigt die Statistik der von APs benutzten Kanäle an.



Hinzufügen zu Falls Sie einen gefundenen AP zur WDS-Konfiguration hinzufügen möchten, geben Sie bitte die MAC-Adresse des APs unten auf der Seite ein und klicken auf Bridge oder Repeater. Dann klicken Sie auf **Hinzufügen zu**. Die MAC-Adresse des APs wird dem Bridge- oder Repeater-Feld auf der WDS-Konfigurationsseite hinzugefügt.

4.11.8 Liste der Clients

Die **Liste der Clients** enthält Informationen über die aktuell verbundenen Clients und den Status-Code. Die Codes werden unten erläutert. Zwecks **Zugriffskontrolle** können Sie einen WLAN-Client wählen und auf **Hinzufügen** klicken.

Wireless LAN >> Liste der Clients

Liste der Clients

Status	MAC-Adresse	verbunden mit

Aktualisieren

Statusdefinitionen :
C: verbunden, keine Verschlüsselung
E: verbunden, WEP
P: verbunden, WPA
A: verbunden, WPA2
B: blockiert durch die Zugriffskontrolle
N: Verbindungsaufbau
F: WPA/PSK Authentifizierung fehlgeschlagen

Hinweis: Ist die WLAN-Verbindung zwischen dem Router und einem Client unterbrochen, wird der WLAN-Client aufgrund von Verzögerungen nicht sofort aus der Liste entfernt.

Hinzufügen zur Zugriffskontrolle :

MAC-Adresse des Clients : : : : :

Hinzufügen

Aktualisieren	Klicken Sie auf diese Taste, um den Status der Client-Liste zu aktualisieren.
Hinzufügen	Klicken Sie auf diese Taste, um die eingegebene MAC-Adresse der **Zugriffskontrolle** hinzuzufügen.

4.12 Systemmanagement

Es gibt verschiedene Bereiche, die für die Konfiguration von Bedeutung sind: Status, Administratorpasswort, Konfigurations-Backup, Syslog, Zeit und Datum, Neustart und Aktualisierung der Firmware.

Die folgende Abbildung zeigt die Menüeinträge für das Systemmanagement:



4.12.1 Systemstatus

Im **Systemstatus** sehen Sie grundlegende Netzwerkeinstellungen des Vigor-Routers. Dies umfasst Informationen über die LAN- und WAN-Schnittstellen. Außerdem werden die aktuelle Version und Informationen bezüglich dieser Firmware angezeigt.

Systemstatus

Modellname	: Vigor2710 series
Firmwareversion	: 3.2.3_2111112
Erstellungsdatum	: Feb 12 2009 18:35:57
ADSL-Modemcode	: 2111112_B Annex A

LAN	
MAC-Adresse	: 00-50-7F-8F-FA-B8
NAT IP-Adresse	: 192.168.1.1
NAT Subnetz-Maske	: 255.255.255.0
DHCP-Server	: Ja
DNS	: 194.109.6.66

WAN	
Verbindungsstatus	: getrennt
MAC-Adresse	: 00-50-7F-8F-FA-B9
Verbindung	: PPPoE
IP-Adresse	: ---
Standard-Gateway	: ---

VoIP			
Port	Profil	Reg.	Rein/Raus
Phone1		Nein	0/0
FXS2		Nein	0/0

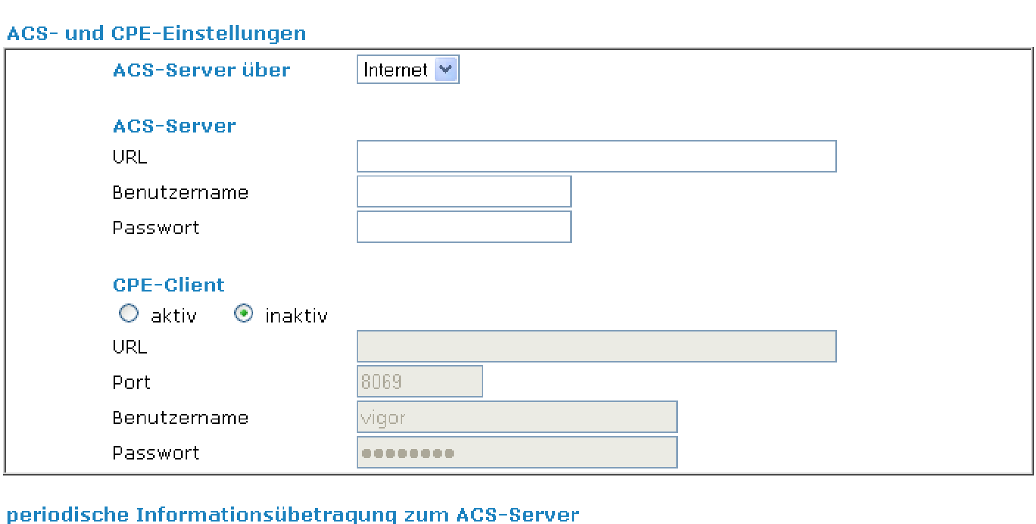
Wireless LAN	
MAC-Adresse	: 00-50-7f-8f-fa-b8
Frequenzbereich	: Europe
Firmwareversion	: 1.8.1.0
SSID	: DrayTek

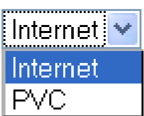
Modellname	Modellname des Routers
Firmwareversion	Firmwareversion des Routers
Erstellungsdatum	Datum und Uhrzeit der Erstellung der aktuellen Firmware
ADSL-Modemcode	ADSL-Firmwareversion
LAN-------	
MAC-Adresse	MAC-Adresse der LAN-Schnittstelle
NAT IP-Adresse	IP-Adresse der LAN-Schnittstelle
Subnetz-Maske	Adresse der Subnetz-Maske der LAN-Schnittstelle
DHCP-Server	Aktueller Status des DHCP-Servers der LAN-Schnittstelle
DNS	Zugewiesene IP-Adresse des bevorzugten DNS-Servers
WAN-------	
Verbindungsstatus	Aktueller Verbindungsstatus
MAC-Adresse	MAC-Adresse der WAN-Schnittstelle

Verbindung	Verbindungsart
IP-Adresse	IP-Adresse der WAN-Schnittstelle
Standard-Gateway	Zugewiesene IP-Adresse des Standard-Gateways
Wireless LAN-------	
MAC-Adresse	MAC-Adresse des Wireless LANs
Frequenzbereich	Zur Auswahl stehen Europa (13 verwendbare Kanäle), USA (11 verwendbare Kanäle), usw. Die von Wireless-Geräten unterstützten Kanäle unterscheiden sich von Land zu Land.
Firmwareversion	Zeigt Informationen zur WLAN Mini-PCI-Karte an. Daraus ergibt sich die Verfügbarkeit einiger Funktionen, die mit der WLAN Mini-PCI-Karte zusammenhängen.
SSID	SSID des Routers

4.12.2 TR-069

Dieses Gerät unterstützt die Norm TR-069. Es ist für einen Administrator sehr bequem, ein TR-069-Gerät über einen Auto-Konfigurationsserver wie VigorACS zu verwalten.



ACS-Server über	Wählen Sie die Schnittstelle, über die der Router mit dem ACS-Server verbunden werden soll. 
ACS-Server	**URL/Benutzername/Passwort –** Diese Daten müssen für den ACS (Auto Configuration Server) eingegeben werden, zu dem Sie eine Verbindung aufbauen möchten. Weitere Einzelheiten sind im Benutzerhandbuch des ACS verfügbar.
CPE-Client	Hier braucht nichts eingegeben zu werden. Die Information ist für den ACS nützlich.

	Aktiv/Inaktiv – Manchmal können Port-Konflikte auftreten. Um solche Probleme zu lösen, können Sie die Port-Nummer für CPE ändern. Klicken Sie auf **Aktiv** und ändern Sie die Port-Nummer.
Periodische Informationsübertragung zum ACS-Server	Die Standardeinstellung ist **Aktiv**. Geben Sie die Intervalle oder Zeiten an, zu denen der Router das CPE benachrichtigen soll. Um die Benachrichtigung zu deaktivieren, klicken Sie auf **Inaktiv**.

4.12.3 Administratorpasswort

Auf dieser Seite können Sie ein neues Passwort setzen:

Systemmanagement >> Administrator-Passwort

Administrator-Passwort

altes Passwort	
neues Passwort	
Passwort bestätigen	

OK

Altes Passwort	Geben Sie das alte Passwort ein. Per Werkseinstellung ist das Passwort "**admin**".
Neues Passwort	Geben Sie das neue Passwort in diesem Feld ein.
Passwort bestätigen	Geben Sie das neue Passwort erneut ein.

Wenn Sie auf OK klicken, erscheint das Anmeldefenster. Bitte benutzen Sie das neue Passwort, um sich erneut im Router-Menü anzumelden.

4.12.4 Sicherung der Konfiguration

Konfiguration sichern

Befolgen Sie die folgenden Schritte, um Ihre Konfiguration zu sichern.

1. Gehen Sie zu **Systemmanagement** >> **Konfiguration sichern**. Das folgende Fenster erscheint wie unten abgebildet.

Systemmanagement >> Konfiguration sichern

Erstellen / Laden eines Backups

Wiederherstellen

Wählen Sie eine Konfigurationsdatei aus.

Durchsuchen...

Klicken Sie auf "Wiederherstellen", um die Datei hochzuladen.

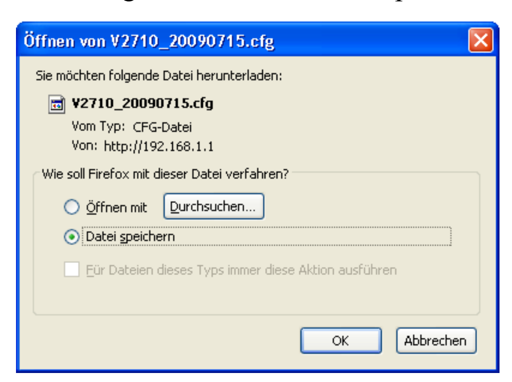
Wiederherstellen

Datensicherung

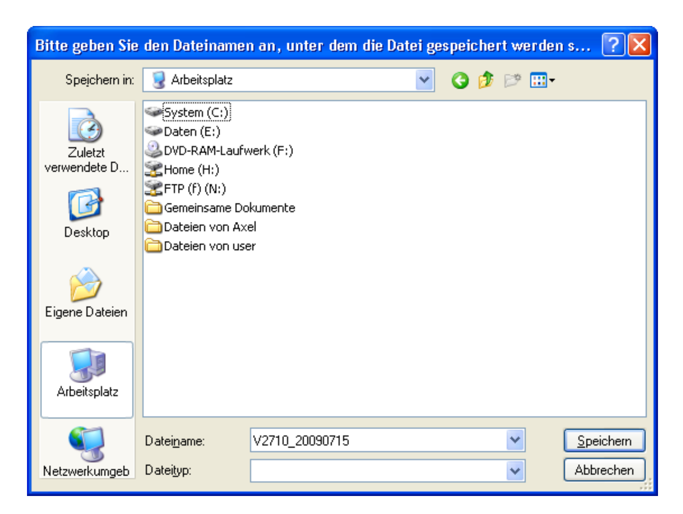
Klicken Sie auf "Datensicherung", um die aktuelle Konfiguration als Datei zu speichern.

Datensicherung Abbrechen

2. Klicken Sie auf **Datensicherung**, um in den folgenden Dialog zu gelangen. Klicken Sie dann auf **Speichern**, um einen weiteren Dialog zu öffnen, in dem Sie die Konfiguration in eine Datei speichern können.



3. Der Standard-Dateinname im Dialog **Speichern unter** ist **config.cfg**. Sie können jedoch einen anderen Namen zuweisen.



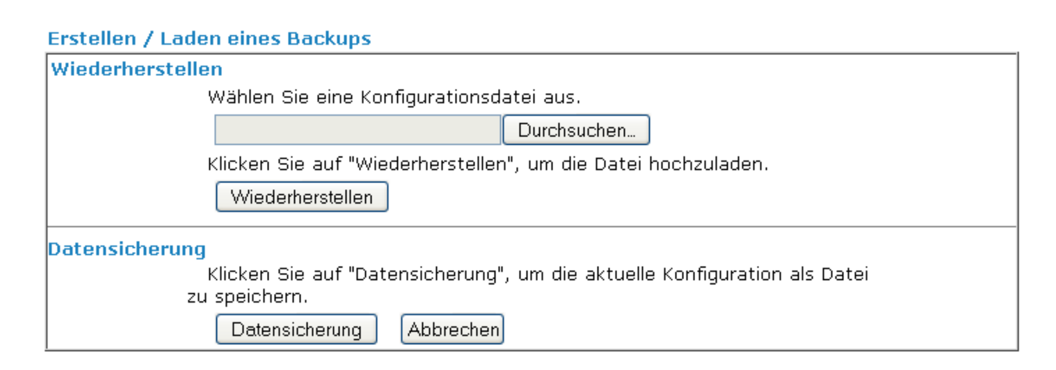
4. Klicken Sie auf **Speichern**, um die Konfiguration automatisch in eine Datei namens **config.cfg** auf Ihren Rechner herunterzuladen.

5. Das obige Beispiel verwendet die **Windows**-Plattform. Die **Mac**- oder **Linux** Plattformen zeigen zwar unterschiedliche Dialoge an, die Sicherungsfunktion ist jedoch trotzdem verfügbar.

Hinweis: Die Zertifikate müssen gesondert gesichert werden. Das Konfigurations-Backup schließt die Zertifikatinformationen nicht ein.

Konfiguration wiederherstellen

1. Gehen Sie zu **Systemmanagement** >> **Konfiguration sichern**. Das folgende Fenster erscheint wie unten abgebildet.



2. Klicken Sie auf **Durchsuchen**, um die für den Router zu ladende Konfigurationsdatei auszuwählen.

3. Klicken Sie auf **Wiederherstellen** und warten Sie ein paar Sekunden, bis das folgende Bild erscheint und bestätigt, dass der Wiederherstellungsprozess erfolgreich war.

4.12.5 Syslog/Mail-Alarm

Die Syslog-Funktion dient der Überwachung des Routers durch den Benutzer. Dank dieser Funktion ist es nicht nötig, sich für die Fehlersuche im Konfigurationsmenü anzumelden.

Systemmanagement >> SysLog und E-Mail Alarm

SysLog und E-Mail Alarm

SysLog-Einstellungen		E-Mail Alarm Einstellungen	
☑ aktiv		☑ aktiv	Test-eMail versenden
Server-IP		IP des SMTP-Servers	
Ziel-Port	514	E-Mail an	
Aktiviere SysLog Meldungen:		Absendeadresse (Reply)	
☑ Firewall-Log		☐ Authentifizierung	
☑ VPN-Log		Benutzername	
☑ Benutzerzugriff-Log		Passwort	
☑ Anruf-Log		E-Mail-Alarm aktivieren für:	
☑ WAN-Log		☑ DoS-Angriffe	
☑ Router/DSL Information		☑ IM und P2P	

OK Löschen Abbrechen

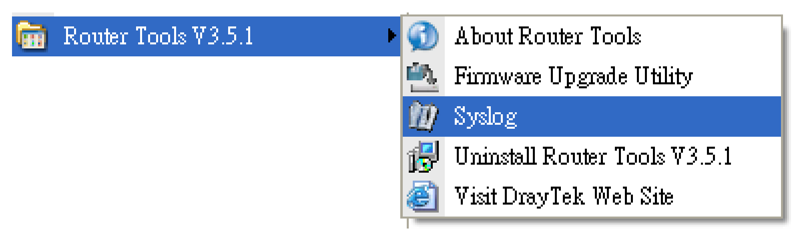
Aktiv (Syslog…)	Markieren Sie **Aktiv**, um die Syslog-Funktion zu aktivieren.
Syslog Server-IP	IP-Adresse des Syslog-Servers.
Ziel-Port	Bestimmen Sie einen Port für das Syslog-Protokoll.
Aktiviere SysLog Meldungen	Markieren Sie das Kästchen auf dieser Web-Seite, um die entsprechenden Meldungen über Firewall, VPN, Benutzerzugriff, Anrufe, WAN und Router/DSL an Syslog zu senden.

Aktiv (Alarmeinstellungen…)	Markieren Sie **Aktiv**, um die Mail-Alarmfunktion zu aktivieren.
Test-E-Mail versenden	Testet die auf dieser Seite angegebene E-Mail-Adresse. Bitte geben Sie zuerst die E-Mail-Adresse an und klicken dann auf diese Taste, um zu überprüfen, ob die E-Mail-Adresse erreichbar ist oder nicht.
SMTP-Server	IP-Adresse des SMTP-Servers.
E-Mail an	Geben Sie eine Mail-Adresse für ausgehende Mails an.
Absendeadresse (Reply)	Geben Sie einen Pfad für eingehende Mails an.
Authentifizierung	Markieren Sie dieses Kästchen, um diese Funktion während der Nutzung der E-Mail-Anwendung zu aktivieren.
Benutzername	Geben Sie den Benutzernamen für die Authentisierung ein.
Passwort	Geben Sie das Authentisierungspasswort ein.
E-Mail-Alarm aktivieren für	Markieren Sie das Kästchen, damit Warnmeldungen an das E-Mail-Postfach gesendet werden, wenn der Router die hier angegebenen Umstände erkennt.

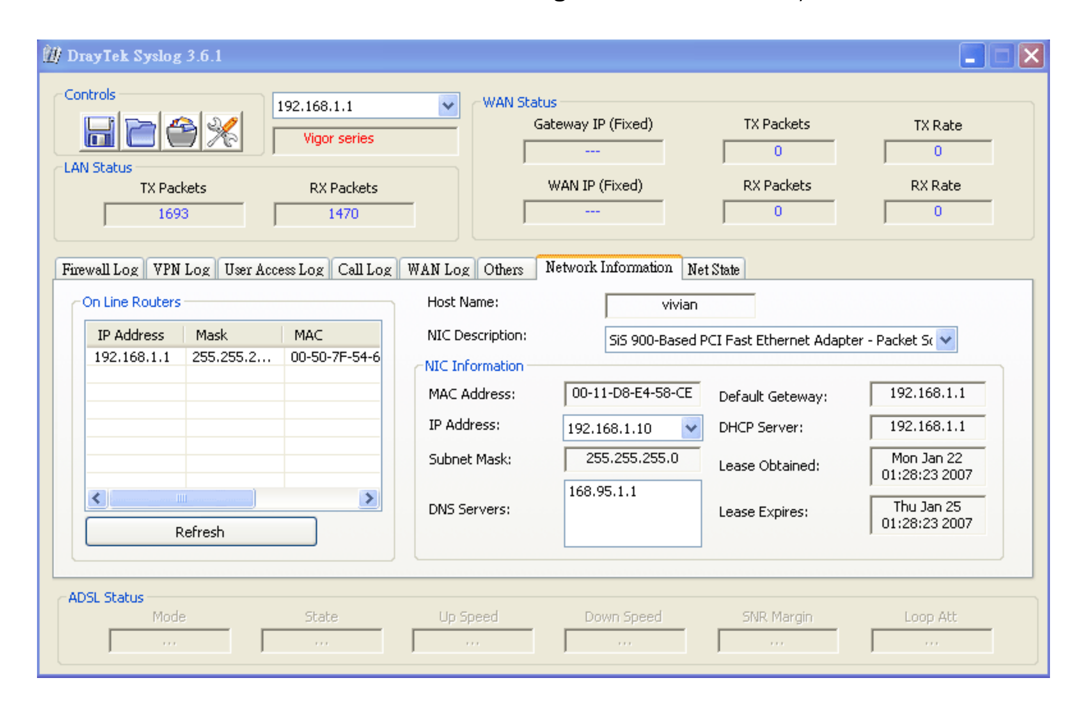
Klicken Sie auf **OK**, um diese Einstellungen zu speichern.

Gehen Sie wie folgt vor, um das Syslog zu betrachten:

1. Geben Sie die IP-Adresse des beobachtenden Rechners im Feld für die Server-IP-Adresse ein.
2. Installieren Sie die Router Tools im **Utility**-Menü auf der mitgelieferten CD. Wählen Sie nach der Installation aus dem Programmmenü **Router Tools>>Syslog**.

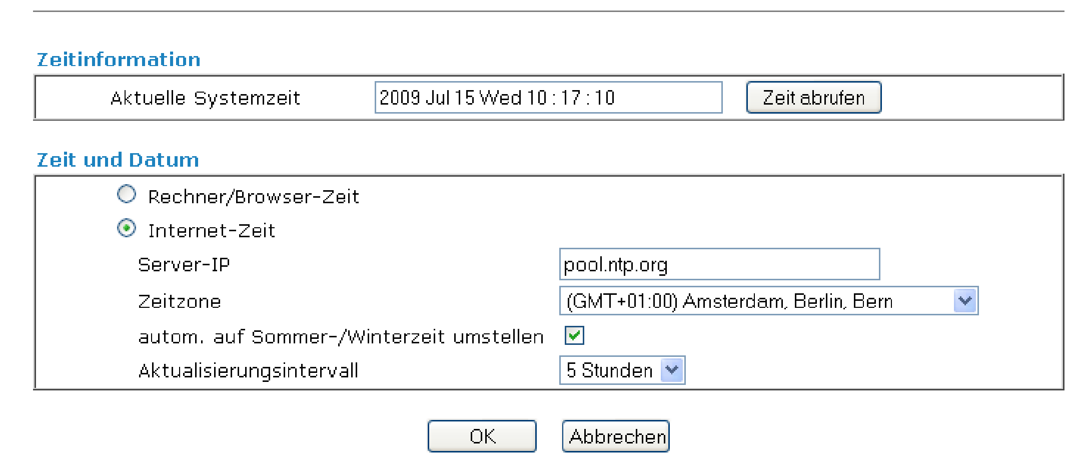


3. Wählen Sie im Syslog-Menü den Router, den Sie überwachen möchten. Dazu müssen Sie unter **Network Information** die Netzwerkkarte wählen, über die der Rechner mit dem Router verbunden ist. Ansonsten können Sie keine Informationen vom Router erhalten.



4.12.6 Zeit und Datum

Hier können Sie angeben, wo der Router die Uhrzeit abfragen soll.



Aktuelle Systemzeit	Klicken Sie auf **Zeit abrufen**, um die aktuelle Zeit zu erhalten.
Rechner-/Browserzeit	Wählen Sie diese Option, um die Browser-Zeit des entfernten Rechners des Administrators als Systemzeit für den Router zu verwenden.
Internet-Zeit	Wählen Sie diese Option, um die Zeit über das gewählte Protokoll von Zeitservern im Internet abzufragen.
Zeitprotokoll	Auswahl des Zeitprotokolls.
Server-IP	IP-Adresse des Zeitservers eingeben.
Zeitzone	Zeitzone auswählen, in der sich der Router befindet.
Aktualisierungs-intervall	Wählen Sie ein Zeitintervall für die Aktualisierung vom NTP-Server.

Klicken Sie auf **OK**, um diese Einstellungen zu speichern.

4.12.7 Verwaltung

Auf dieser Seite können Sie die Einstellungen zur Zugriffskontrolle, Zugriffsliste, Port-Konfiguration und SNMP-Konfiguration verwalten.

Systemmanagement >> Verwaltung

Systemverwaltung

Zugangsverwaltung

- ☑ Management aus dem Internet erlauben
  - ☐ FTP-Server
  - ☑ HTTP-Server
  - ☑ HTTPS-Server
  - ☑ Telnet-Server
  - ☐ SSH-Server
- ☑ Router ignoriert PING aus dem Internet

Zugangsberechtigung

Nr.	IP-Adresse	Subnetz-Maske
1		
2		
3		

Port-Einstellungen verwalten

◉ benutzerdefinierte Ports ○ Standard-Ports

Telnet-Port	23	(Standard: 23)
HTTP-Port	80	(Standard: 80)
HTTPS-Port	443	(Standard: 443)
FTP-Port	21	(Standard: 21)
SSH-Port	22	(Standard: 22)

SNMP-Einstellungen

☐ SNMP aktiv

Get Community	public
Set Community	private
IP des Host-Managers	
Trap Community	public
Benachrichtigung an IP	
Timeout für Trap	10 Sekunden

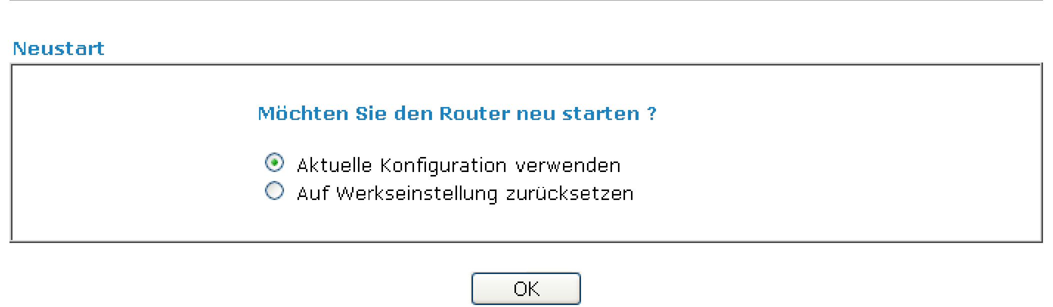
OK

Management aus dem Internet erlauben	Aktivieren Sie dieses Kästchen, um Systemadministratoren zu ermöglichen, sich aus dem Internet anzumelden. Das System bietet verschiedene Server, um den Router aus dem Internet zu verwalten. Haken Sie das/die entsprechenden Kästchen an.
Router ignoriert PING aus dem Internet	Aktivieren Sie dieses Kästchen, um alle Ping-Pakete aus dem Internet zu verwerfen. Diese Funktion ist aus Sicherheitsgründen standardmäßig aktiviert.
Zugangsberechtigung	Sie können bestimmen, dass sich der Systemadministrator nur von einem in der Liste angegebenen Host oder Network anmelden kann. Es können bis zu drei IPs/Subnetz-Masken angegeben werden. **Nr. IP** - Zeigt eine IP-Adresse an, der gestattet wird, sich am Router anzumelden. **Subnetz-Maske -** Zeigt eine Subnetz-Maske an, der gestattet wird, sich am Router anzumelden.
Standard-Ports	Markieren, um die Standard-Port-Nummern für die Telnet- und HTTP-Server zu verwenden.
Benutzerdefinierte Ports	Markieren, um benutzerdefinierte Portnummern für die Telnet-, HTTP- und FTP-Server anzugeben.
SNMP aktiv.	Markieren, um diese Funktion zu aktivieren.
Get Community	Geben Sie einen Namen für die Get Community ein. Die Standardeinstellung ist **public.**
Set Community	Geben Sie einen Namen für die Community ein. Die Standardeinstellung ist **private.**

IP des Host-Managers	Bestimmen Sie einen Host als Manager, um die SNMP-Funktion auszuführen. Geben Sie die IP-Adresse des Hosts ein.
Trap Community	Geben Sie einen Namen für die Trap Community ein. Die Standardeinstellung ist **public.**
Benachrichtigung an IP	Geben Sie die IP-Adresse des Hosts an, der die Trap Community erhalten soll.
Timeout für Trap	Die Standardeinstellung ist 10 Sekunden.

4.12.8 Neustart

Der Router kann aus dem Konfigurationsmenü heraus neu gestartet werden. Wählen Sie **Neustart** unter **Systemmanagement**, um die folgende Seite zu öffnen:



Falls Sie den Router mit der aktuellen Konfiguration neu starten möchten, wählen Sie **Aktuelle Konfiguration verwenden** und klicken auf **OK**. Um den Router auf die Werkseinstellungen zurückzusetzen, wählen Sie **Auf Werkseinstellung zurücksetzen** und klicken auf **OK**. Der Router benötigt fünf Sekunden, um das System neu zu starten.

Hinweis: Wenn das System nach Konfiguration der Internet-Einstellungen die Web-Seite für den Neustart des Systems anzeigt, klicken Sie bitte auf **OK**, um Ihren Router neu zu starten und so den ordnungsgemäßen Betrieb sicherzustellen und unerwartete Router-Probleme in der Zukunft zu vermeiden.

4.12.9 Firmware aktualisieren

Um Ihre Router-Firmware zu aktualisieren müssen Sie die Router Tools installieren. Das **Firmware Upgrade Utility** ist in den Tools enthalten. Die folgende Web-Seite erläutert die Aktualisierung der Firmware anhand eines Beispiels. Das Beispiel verwendet das Windows-Betriebssystem.

Laden Sie die neueste Firmware von der DrayTek-Web-Site oder -FTP-Site herunter. Die Draytek-Web-Site ist www.draytek.de, und die FTP-Site ist ftp.draytek.com.

Wählen Sie **Systemmanagement>> Firmware aktualisieren**, um das Firmware Upgrade Utility zu starten.

Systemmanagement >> Firmware aktualisieren

Online Firmware-Upgrade

Wählen Sie eine Firmware Datei.

[ ] Durchsuchen...

Klicken Sie Upgrade, um die Firmware hochzuladen. Upgrade

TFTP Firmware-Upgrade von LAN

aktuelle Firmwareversion: 3.2.3_2111112

Firmware-Upgrade Prozedur:

1. Unten durch Bestätigen des "OK"-Buttons den TFTP-Server starten.
2. Starten von DrayTek's Firmware-Upgrade-Utility oder einer anderen TFTP-Software.
3. Firmwaredatei auswählen.
4. Datei an Router senden.
5. Der TFTP-Server wird nach dem Download automatisch beendet.

Möchten Sie die Firmware aktualisieren? OK

Klicken Sie auf **OK**. Der folgende Dialog erscheint. Bitte führen Sie zunächst die Firmware-Aktualisierung durch.

Systemmanagement >> Firmware aktualisieren

Der TFTP-Server läuft. Bitte starten Sie eine Firmware-Upgrade-Software, um die Router-Firmware zu aktualisieren. Dieser Server schließt sich selbstständig, sobald das Firmware-Upgrade beendet ist.

Einzelheiten zur Aktualisierung der Firmware werden in Kapitel 4 erläutert.

4.13 Diagnose-Tools

Die Diagnose-Tools eignen sich zur **Kontrolle** oder **Diagnose** des Status Ihres Vigor-Routers.

Die folgende Abbildung zeigt die Menüeinträge für die Diagnose-Tools:

Diagnose-Tools
- Anwahlauslöser
- Routing-Tabelle
- ARP-Cache-Tabelle
- DHCP-Tabelle
- NAT-Tabelle
- Datenfluss-Monitor
- Traffic-Diagramm
- Ping
- Trace Route

4.13.1 Anwahlauslöser

Wählen Sie **Diagnose-Tools** und klicken auf **Anwahlauslöser**, um die Web-Seite zu öffnen. Die Internet-Verbindung (z.B. PPPoE, PPPoA usw.) wird von einem Paket von der Quell-IP-Adresse angestoßen.

Diagnose-Tools >> Anwahlauslöser

Anwahlauslösender Paket-Header | Aktualisieren |

HEX-Format:

```
00 50 7F 8F FA B8-00 18 37 05 1B AC-08 00

45 00 00 41 7F CC 00 00-7F 11 31 7E C0 A8 01 0A
C2 6D 06 42 FC F4 00 35-00 2D 1F 5D 29 75 01 00
00 01 00 00 00 00 00 00-03 77 77 77 0B 73 74 6F
70 62 61 64 77 61 72 65-03 6F 72 67 00 00 01 00
01 DF 00 00 00 63 80 ED-2B AF 80 4A FA 14 43 00
```

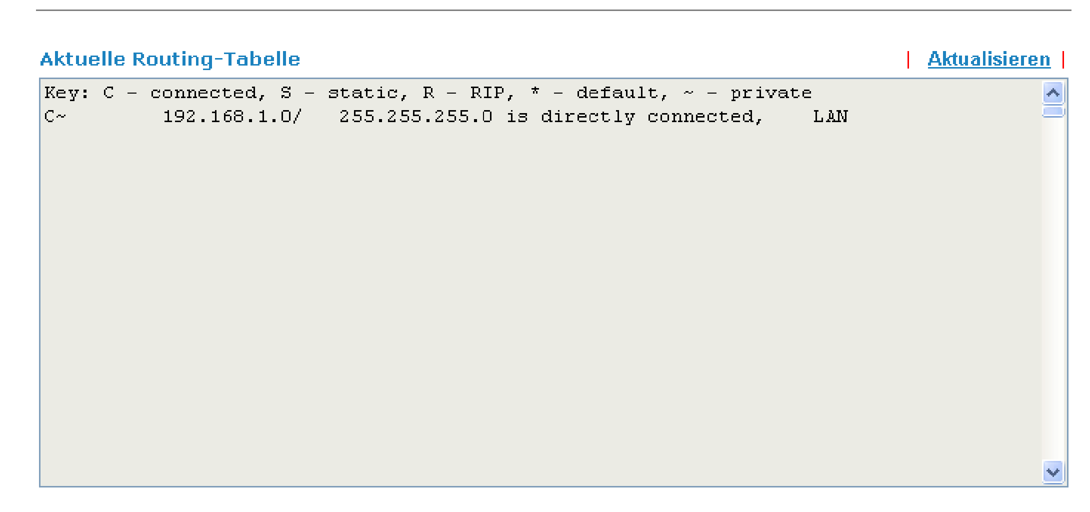
Klartext:

```
192.168.1.10,64756 -> 194.109.6.66,domain
Pr UDP HLen 20 TLen 65
```

Klartext	Zeigt die Quell-IP-Adresse (lokal), die Ziel-IP-Adresse (entfernt), das Protokoll und die Länge des Pakets an.
Aktualisieren	Anklicken, um die Seite neu zu laden.

4.13.2 Routing-Tabelle

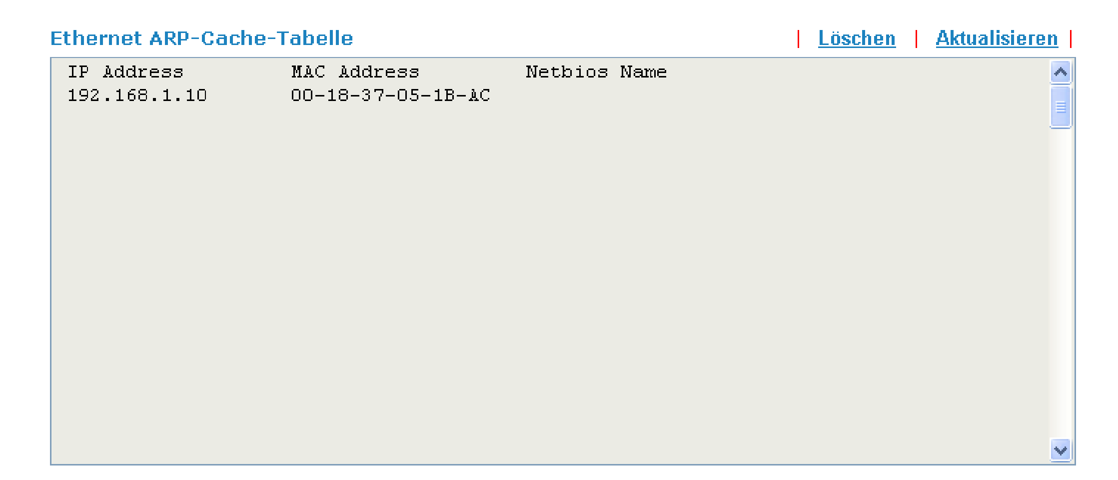
Wählen Sie **Diagnose-Tools** und klicken auf **Routing-Tabelle**, um die Web-Seite zu öffnen.



Aktualisieren Anklicken, um die Seite neu zu laden.

4.13.3 ARP-Cache-Tabelle

Klicken Sie auf **Diagnose-Tools** und wählen Sie **ARP-Cache-Tabelle**, um den Inhalt des ARP-Caches (Address Resolution Protocol) im Router zu betrachten. Die Tabelle zeigt die Zuordnung zwischen den Ethernet-Hardware-Adressen (MAC-Adressen) und IP-Adressen an.



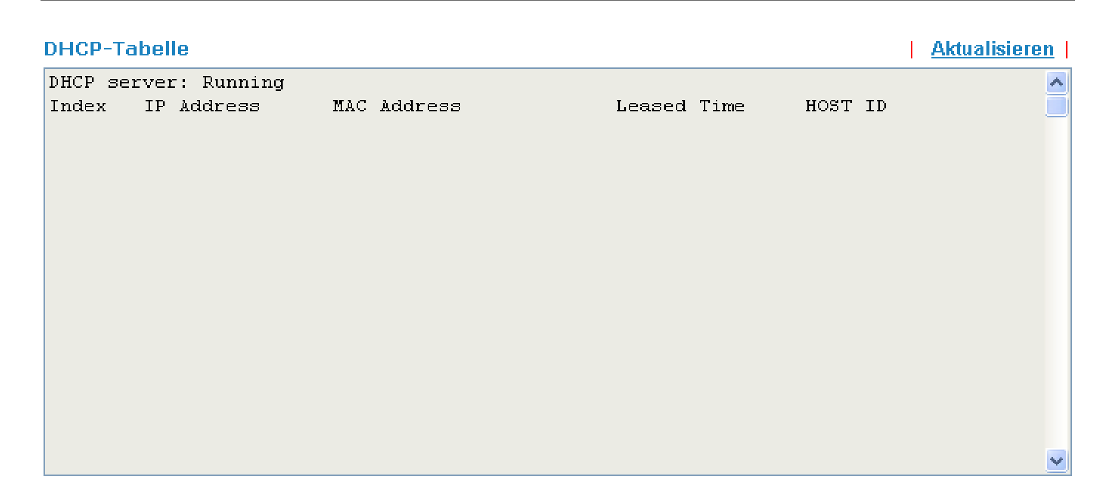
Aktualisieren	Anklicken, um die Seite neu zu laden.
Löschen	Anklicken, um die gesamte Tabelle zu löschen.

4.13.4 DHCP-Tabelle

Diese Tabelle liefert Informationen zur Zuweisung von IP-Adressen. Diese Informationen sind nützlich für die Diagnose von Netzwerkproblemen wie IP-Adressenkonflikte usw.

Wählen Sie **Diagnose-Tools** und klicken auf **DHCP-Tabelle**, um die Web-Seite zu öffnen.

Diagnose-Tools >> DHCP-Tabelle

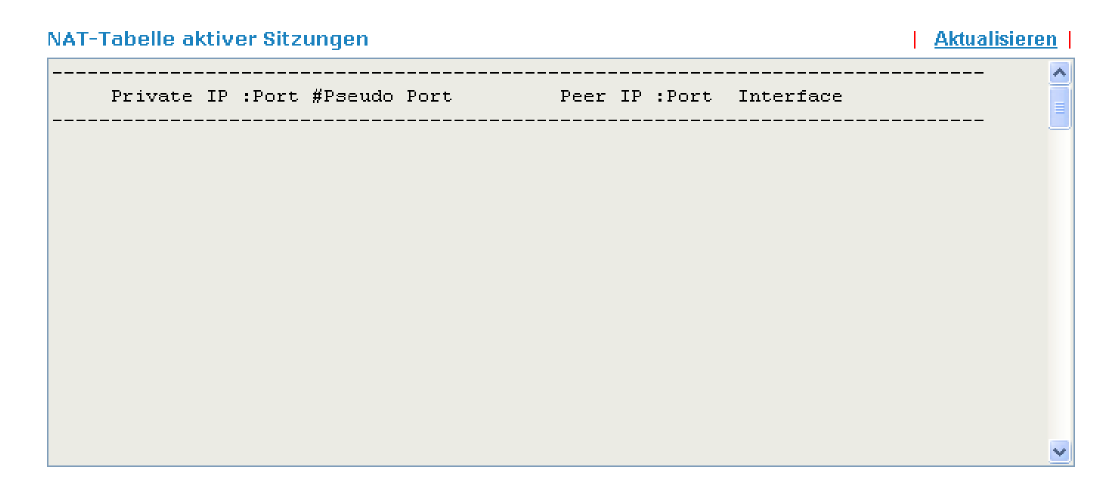


Index	Zeigt die Verbindungsnummer an.
IP-Adresse	Zeigt die IP-Adresse an, die dieser Router dem angegebenen Rechner zugewiesen hat.
MAC-Adresse	Zeigt die MAC-Adresse des angegebenen Rechners an, der DHCP eine IP-Adresse zugewiesen hat.
Lease Time	Zeigt die Lease Time des angegebenen Rechners an.
Host ID	Zeigt die Host-ID des angegebenen Rechners an.
Aktualisieren	Anklicken, um die Seite neu zu laden.

4.13.5 NAT-Sitzungstabelle

Wählen Sie **Diagnose-Tools** und klicken auf **NAT-Tabelle**, um die Seite mit der Liste zu öffnen.

Diagnose-Tools >> NAT-Tabelle



Private IP:Port	Gibt die Quell-IP-Adresse und den Port des lokalen Rechners an.
#Pseudo-Port	Gibt den zeitweiligen Port des Routers an, der für NAT verwendet wird.
Peer-IP:Port	Zeigt die Ziel-IP-Adresse und den Port des entfernten Hosts an.
Schnittstelle	Zeigt die entsprechende Nummer der Schnittstelle an.
Aktualisieren	Anklicken, um die Seite neu zu laden.

4.13.6 Datenfluss-Monitor

Diese Seite zeigt die Aktivität der überwachten IP-Adresse an und aktualisiert die Daten alle paar Sekunden. Die hier angezeigte IP-Adresse wird im Bandbreitenmanagement konfiguriert. Sie müssen IP-Bandbreitenbegrenzung und IP-Sitzungsbegrenzung aktivieren, bevor Sie den Datenfluss-Monitor starten. Falls dies nicht bereits geschehen ist, erscheint eine Meldung, die Sie daran erinnert.

Wählen Sie **Diagnose-Tools** und klicken auf **Datenfluss-Monitor**, um die Web-Seite zu öffnen. Klicken Sie auf **IP-Adresse**, **TX-Rate**, **RX-Rate** oder **Sitzungen**, um sich die entsprechenden Daten anzeigen zu lassen.

Diagnose-Tools >> Datenfluss-Monitor

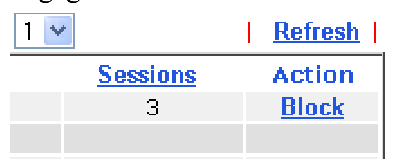
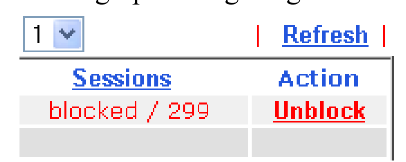
☑ Datenfluss-Monitor aktiv

Aktualisierungsintervall: 10   Seite: 1 | Aktualisieren |

Index	IP-Adresse	TX-Rate(kbit/s)	RX-Rate(kbit/s)	Sitzungen	Aktion

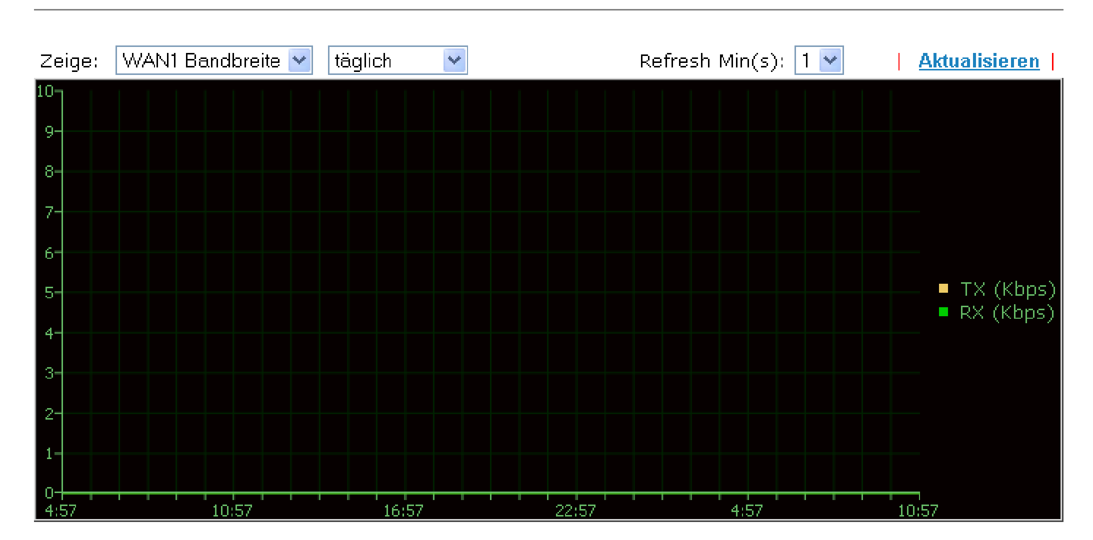
Hinweis: 1. Klicken Sie auf "Blockieren", um den jeweiligen PCs den Zugang zum Internet für 5 Minuten zu verweigern.
2. Die vom Router blockierte IP-Adresse wird rot angezeigt. Die Spalte "Sitzungen" gibt die verbleibende Zeit an, solange die ausgewählte IP noch blockiert wird.

Datenfluss-Monitor aktiv	Markieren Sie dieses Kästchen, um diese Funktion zu aktivieren.
Aktualisierungsintervall	Verwenden Sie die Dropdown-Liste, um das automatische Aktualisierungsintervall (in Sekunden) des Datenfluss-Monitors zu bestimmen. Aktualisierungsintervall: 10 (10, 15, 30)
Aktualisieren	Klicken Sie auf diesen Link, um diese Seite manuell zu aktualisieren.
Index	Nummer des Datenflusses anzeigen.

IP-Adresse	IP-Adresse des überwachten Geräts anzeigen.
Übertragungsgeschwindigkeit (kbps)	Übertragungsgeschwindigkeit des überwachten Geräts anzeigen.
Empfangsgeschwindigkeit (kbps)	Empfangsgeschwindigkeit des überwachten Geräts anzeigen.
Sitzungen	Zeigt die Anzahl der Sitzungen an, die Sie unter Sitzungen begrenzen angegeben haben.
Aktion	**Blockieren** - Sperrt den Internetzugang für den angegebenen PC in fünf Minuten.  **Freigeben** – Das Gerät mit der IP-Adresse wird in fünf Minuten freigegeben. Die verbleibende Zeit wird in der Sitzungsspalte angezeigt. 

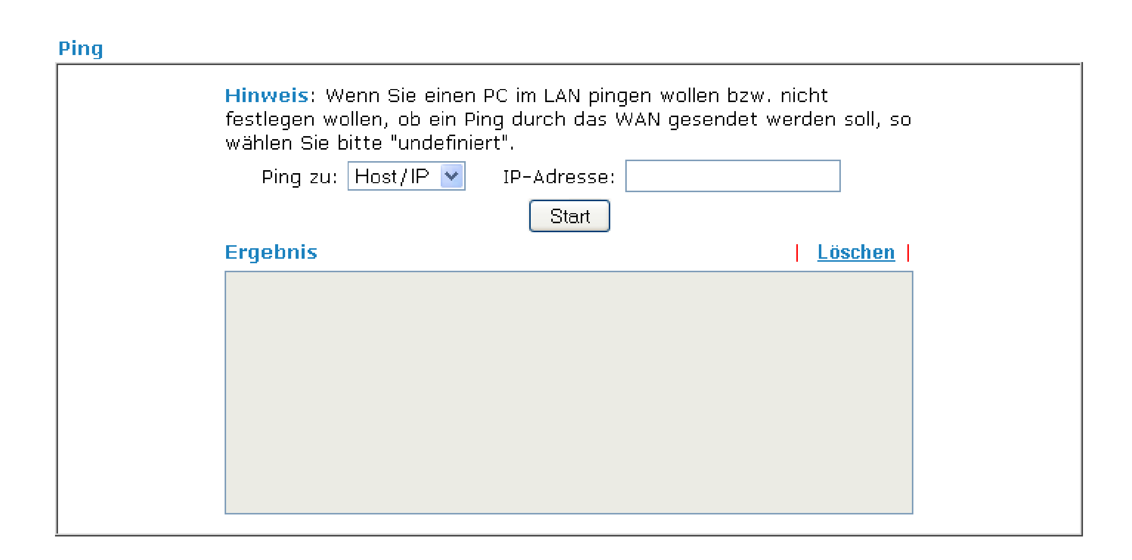
4.13.7 Traffic-Diagramm

Wählen Sie **Diagnose-Tools** und klicken auf **Traffic-Diagramm**, um die Web-Seite zu öffnen. Sie können WAN1 Bandbreite, Sitzungen, täglich oder wöchentlich wählen, um verschiedene Traffic-Diagramme zu betrachten. Sie können jederzeit auf **Aktualisieren** klicken, um das Diagramm zu aktualisieren.



4.13.8 Ping

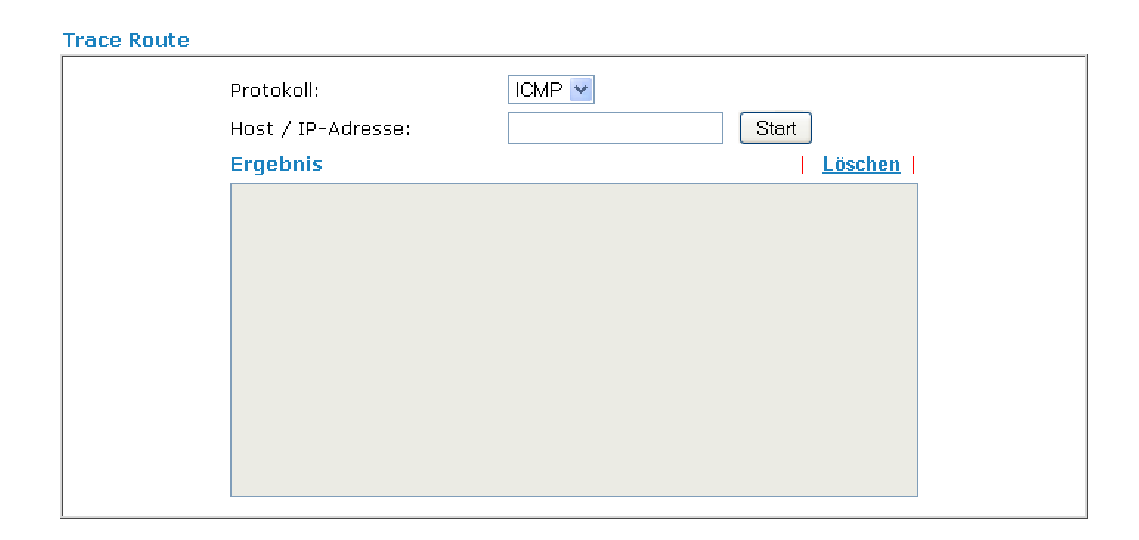
Wählen Sie **Diagnose-Tools** und klicken auf **Ping**, um die Web-Seite zu öffnen.



Ping zu	Verwenden Sie die Dropdown-Liste, um das Ziel zu wählen, das Sie anpingen möchten.
IP-Adresse	Geben Sie die IP-Adresse des Hosts ein, den Sie anpingen möchten.
Start	Klicken Sie auf diese Schaltfläche, um Ping zu starten. Das Ergebnis wird auf dem Bildschirm angezeigt.
Löschen	Klicken Sie auf diesen Link, um die Ausgabe im Fenster zu löschen.

4.13.9 Trace Route

Wählen Sie **Diagnose-Tools** und klicken auf **Trace Route**, um die Web-Seite zu öffnen. Auf dieser Seite können Sie den Pfad vom Router zum Host nachverfolgen. Geben Sie einfach die IP-Adresse des Hosts im Feld ein und klicken auf **Ausführen**. Das Ergebnis wird auf dem Bildschirm angezeigt.



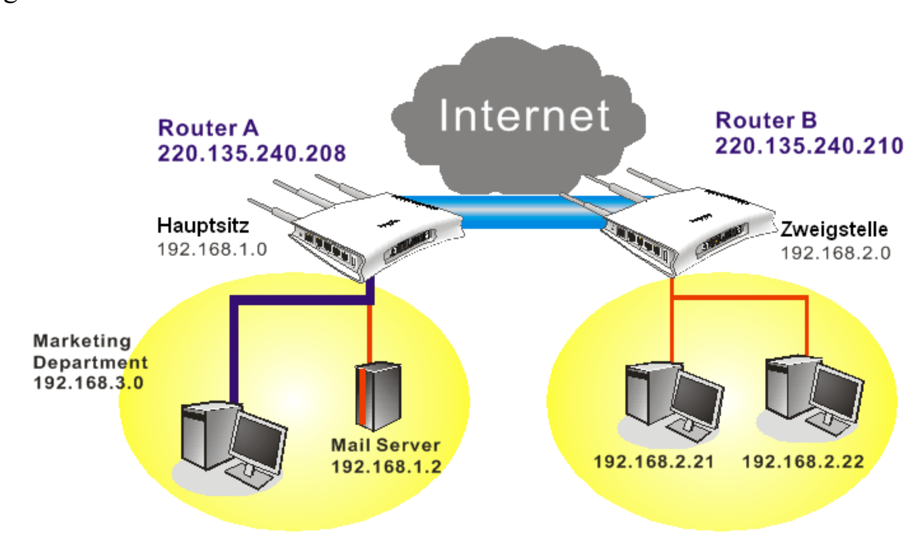
Protokoll	Verwenden Sie die Dropdown-Liste, um die Schnittstelle zu wählen, durch die Sie pingen möchten.
Host/IP-Adresse	Zeigt die Host-IP-Adresse an.
Start	Klicken Sie auf diese Taste, um Trace Route zu starten.
Löschen	Klicken Sie auf diesen Link, um die Ausgabe im Fenster zu löschen.



5 Anwendung und Beispiele

5.1 LAN-zu-LAN-Verbindung zwischen Filiale und Zentrale einrichten

Das häufigste Szenario besteht darin, dass Sie eine sichere Netzwerkverbindung einrichten möchten, beispielsweise zwischen einer Filiale und der Zentrale. Um die abgebildete Netzwerkstruktur einzurichten, befolgen Sie die folgenden Schritte und erstellen ein LAN-zu-LAN-Profil. Diese beiden Netzwerke (LANs) sollten NICHT die gleiche Netzwerkadresse haben.



Einstellungen auf Router A in der Zentrale:

1. Gehen Sie zu **VPN und externe Einwahl**, wählen Sie **Einwahlmöglichkeiten**, um den erforderlichen VPN-Dienst zu ermöglichen, und klicken Sie auf **OK**.
2. Um **PPP**-basierte Dienste wie PPTP oder L2TP zu verwenden, konfigurieren Sie die allgemeinen Einstellungen unter **PPP-Einstellungen**.

VPN und externe Einwahl >> PPP-Einstellungen

PPP-Einstellungen

PPP/MP-Protokoll		IP-Adressenzuweisung für die einwählenden Benutzer (wenn DHCP-Server inaktiv)	
PPP-Authentifizierung beim Einwählen	PAP oder CHAP	IP-Adressbereich zuweisen	192.168.1.200
PPP-Verschlüsselung (MPPE) beim Einwählen	optional		
Gegenseitige Authentifizierung (PAP)	○ Ja ⦿ Nein		
Benutzername			
Passwort			

OK

Um **IPSec**-basierte Dienste wie IPSec oder L2TP mit IPSec zu verwenden, konfigurieren Sie die Einstellungen in **IPSec-Grundeinstellungen**, z.B. den Pre-Shared Key, den beide Seiten kennen.

VPN und externe Einwahl >> IPSec Grundeinstellungen

IKE/IPSec Grundeinstellungen

Einstellungen für die Einwahl in diesen Router von außen (LAN-zu-LAN).

IKE-Authentifizierungsmethode

Pre-Shared Key

Pre-Shared Key bestätigen

IPSec-Sicherheitsmethode

☑ Mittel (AH)

Daten werden authentifiziert, aber nicht verschlüsselt.

Hoch (ESP) ☑ DES ☑ 3DES ☑ AES

Daten werden sowohl authentifiziert als auch verschlüsselt.

OK Abbrechen

3. Gehen Sie zu **LAN zu LAN**. Klicken Sie auf eine der Indexnummern, um ein Profil zu bearbeiten.
4. Konfigurieren Sie die **Allgemeinen Einstellungen** wie unten gezeigt. Aktivieren Sie beide VPN-Verbindungen, damit jede Partei die VPN-Verbindung starten kann.

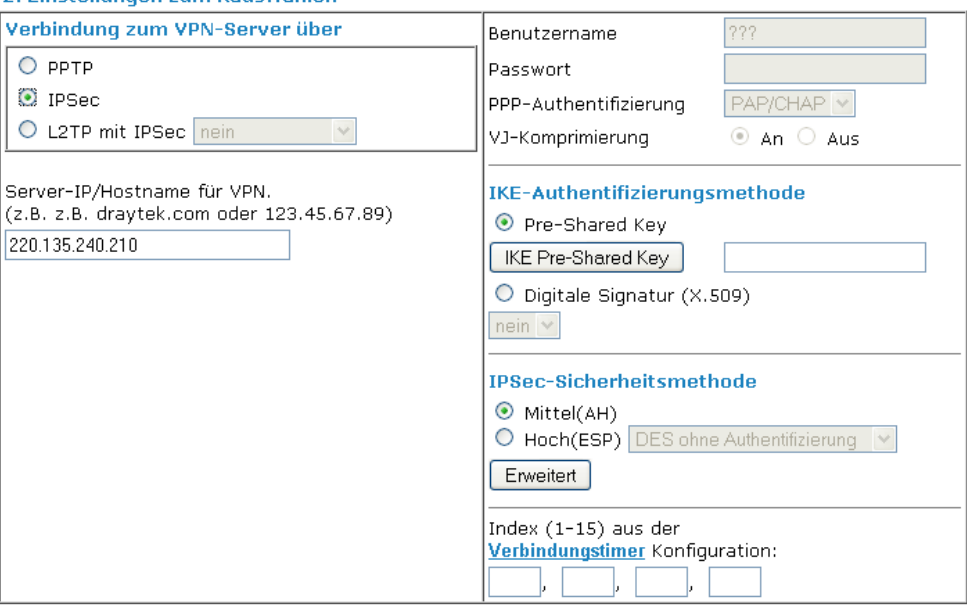
VPN und externe Einwahl >> LAN-zu-LAN

Profil-Index : 1

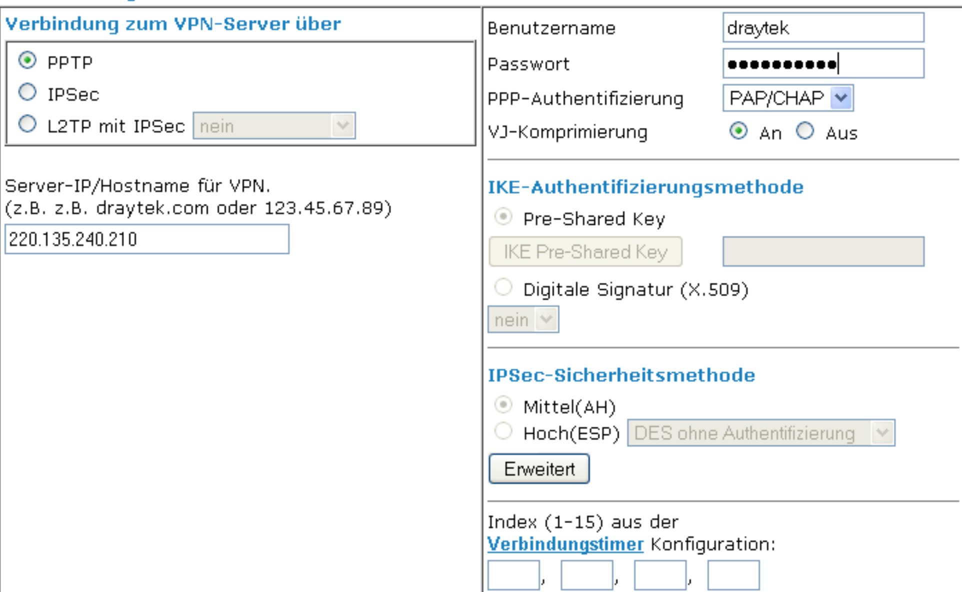
1. Allgemeine Einstellungen

Profilname: Mannheim1	Anrufrichtung: ◉ Beide ○ Raus ○ Dial-in
☑ aktiv	☐ immer in Betrieb
NetBIOS-Name durchlassen ◉ ja ○ nein	Max. Leerlaufzeit 300 Sekunden
	☐ Dauer-Ping aktiv
	Ping an die IP

5. Konfigurieren Sie die **Einstellungen zum Rauswählen** wie unten gezeigt, um den Router B über die gewählte Anwahlmethode aggressiv anzuwählen.
   Bei Auswahl eines ***IPSec-basierten*** Dienstes müssen Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Anwahlverbindung angeben.

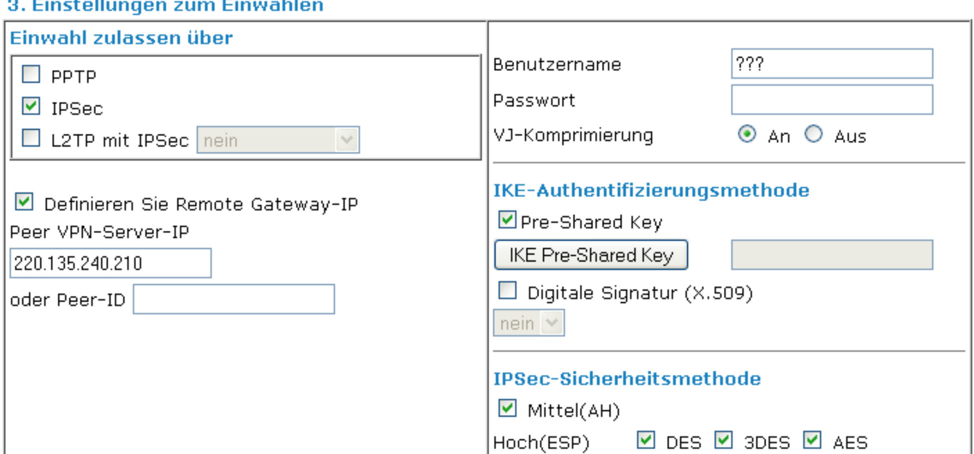


Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort, PPP-Authentifizierung und VJ-Komprimierung für diese Anwahlverbindung angeben.



6. Konfigurieren Sie die **Einstellungen zum Einwählen** wie unten abgebildet, um Router B die Einwahl zum Aufbau einer VPN-Verbindung zu ermöglichen.

   Bei Auswahl eines ***IPSec-basierten*** Dienstes können Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Einwahlverbindung angeben. Ansonsten werden die obigen **IPSec Grundeinstellungen** verwendet.



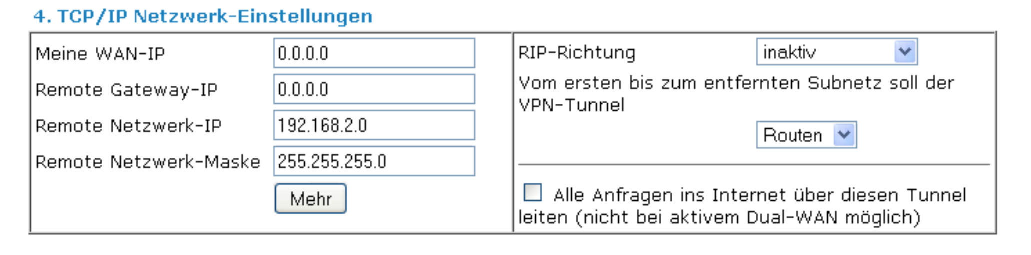
Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort und VJ-Komprimierung für diese Einwahlverbindung angeben.

3. Einstellungen zum Einwählen

Einwahl zulassen über
PPTP
IPSec
L2TP mit IPSec nein
Definieren Sie Remote Gateway-IP
Peer VPN-Server-IP
220.135.240.210
oder Peer-ID

Benutzername draytek
Passwort ●●●●●●●●●●●
VJ-Komprimierung An Aus
IKE-Authentifizierungsmethode
Pre-Shared Key
IKE Pre-Shared Key
Digitale Signatur (X.509)
nein
IPSec-Sicherheitsmethode
Mittel(AH)
Hoch(ESP) DES 3DES AES

7. Schließlich konfigurieren Sie die entfernte Netzwerk-IP/das entfernte Subnetz in **TCP/IP-Netzwerkeinstellungen** so, dass der Router A die an Router B im entfernten Netzwerk bestimmten Pakete über die VPN-Verbindung übertragen kann.



Einstellungen auf dem Router B im entfernten Büro:

1. Gehen Sie zu **VPN und externe Einwahl**, wählen Sie **Einwahlmöglichkeiten**, um den erforderlichen VPN-Dienst zu ermöglichen, und klicken Sie auf **OK**.

2. Um **PPP**-basierte Dienste wie PPTP oder L2TP zu verwenden, konfigurieren Sie die allgemeinen Einstellungen unter **PPP-Einstellungen**.

VPN und externe Einwahl >> PPP-Einstellungen

PPP-Einstellungen

PPP/MP-Protokoll
PPP-Authentifizierung beim Einwählen PAP oder CHAP
PPP-Verschlüsselung (MPPE) beim Einwählen optional
Gegenseitige Authentifizierung (PAP)
Ja Nein
Benutzername
Passwort

IP-Adressenzuweisung für die einwählenden Benutzer
(wenn DHCP-Server inaktiv)
IP-Adressbereich zuweisen 192.168.1.200

OK

Um **IPSec**-basierte Dienste wie IPSec oder L2TP mit IPSec zu verwenden, konfigurieren Sie die Einstellungen in **IPSec-Grundeinstellungen**, z.B. den Pre-Shared Key, den beide Seiten kennen.

VPN und externe Einwahl >> IPSec Grundeinstellungen

IKE/IPSec Grundeinstellungen

Einstellungen für die Einwahl in diesen Router von außen (LAN-zu-LAN).

IKE-Authentifizierungsmethode

Pre-Shared Key ●●●●●●●●●●

Pre-Shared Key bestätigen ●●●●●●●●●●

IPSec-Sicherheitsmethode

☑ Mittel (AH)

Daten werden authentifiziert, aber nicht verschlüsselt.

Hoch (ESP) ☑ DES ☑ 3DES ☑ AES

Daten werden sowohl authentifiziert als auch verschlüsselt.

OK Abbrechen

3. Gehen Sie zu **LAN zu LAN**. Klicken Sie auf eine der Indexnummern, um ein Profil zu bearbeiten.
4. Konfigurieren Sie die **Allgemeinen Einstellungen** wie unten gezeigt. Aktivieren Sie beide VPN-Verbindungen, damit jede Partei die VPN-Verbindung starten kann.

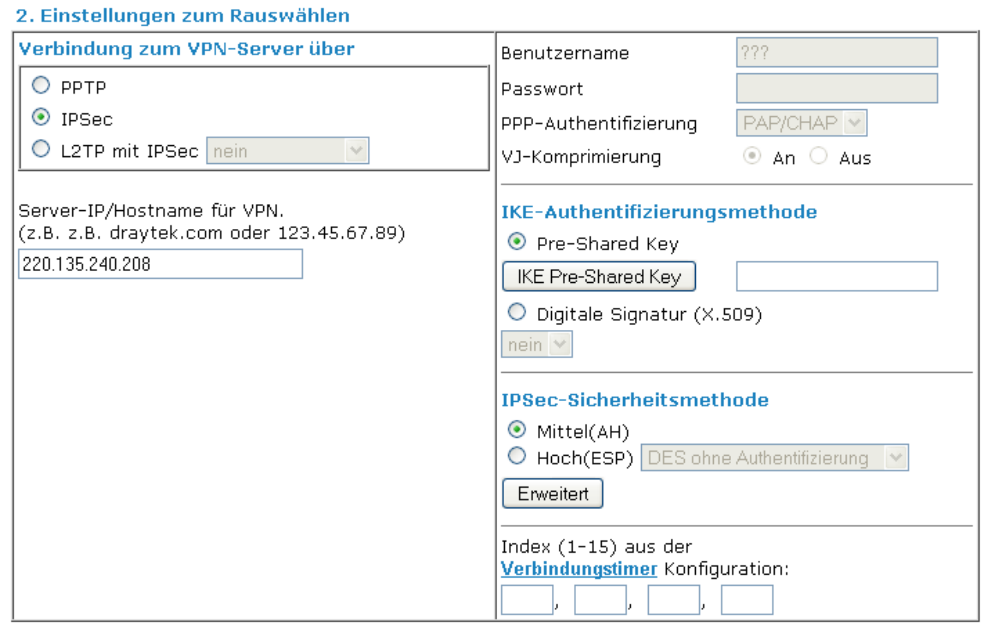
VPN und externe Einwahl >> LAN-zu-LAN

Profil-Index : 1

1. Allgemeine Einstellungen

Profilname Mannheim1	Anrufrichtung: ◉ Beide ○ Raus ○ Dial-in
☑ aktiv	☐ immer in Betrieb
NetBIOS-Name durchlassen ◉ ja ○ nein	Max. Leerlaufzeit 300 Sekunden
	☐ Dauer-Ping aktiv
	Ping an die IP

5. Konfigurieren Sie die **Einstellungen zum Rauswählen** wie unten gezeigt, um den Router B über die gewählte Anwahlmethode aggressiv anzuwählen.



Bei Auswahl eines ***IPSec-basierten*** Dienstes müssen Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Anwahlverbindung angeben.

Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort, PPP-Authentifizierung und VJ-Komprimierung für diese Anwahlverbindung angeben.

2. Einstellungen zum Rauswählen

Verbindung zum VPN-Server über
PPTP
IPSec
L2TP mit IPSec nein

Server-IP/Hostname für VPN.
(z.B. z.B. draytek.com oder 123.45.67.89)
220.135.240.208

Benutzername draytek
Passwort ●●●●●●●●●●
PPP-Authentifizierung PAP/CHAP
VJ-Komprimierung An Aus

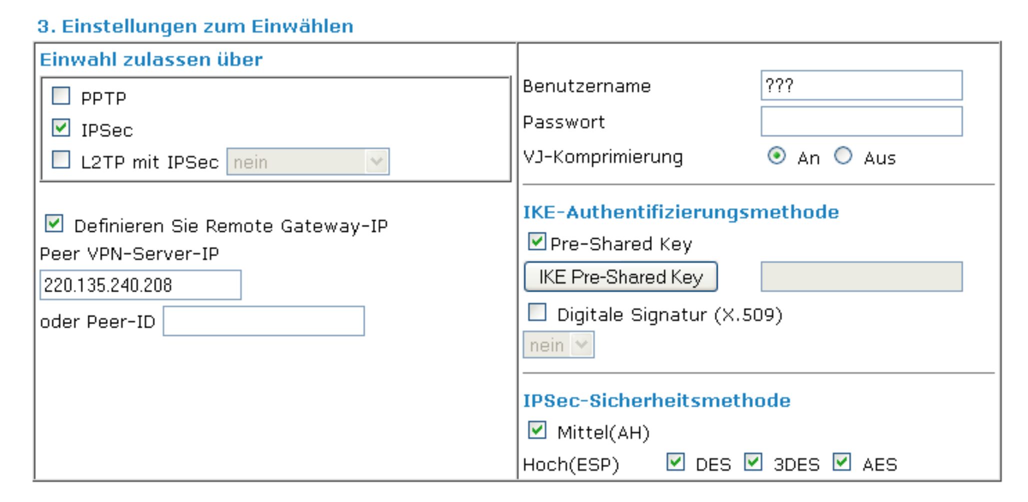
IKE-Authentifizierungsmethode
Pre-Shared Key
IKE Pre-Shared Key
Digitale Signatur (X.509)
nein

IPSec-Sicherheitsmethode
Mittel(AH)
Hoch(ESP) DES ohne Authentifizierung
Erweitert

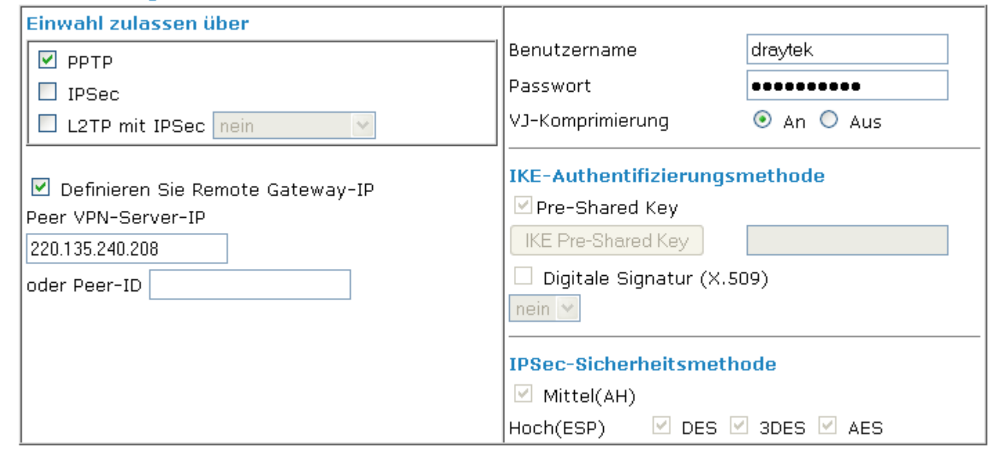
Index (1-15) aus der Verbindungstimer Konfiguration:

6. Konfigurieren Sie die **Einstellungen zum Einwählen** wie unten abgebildet, um Router A die Einwahl zum Aufbau einer VPN-Verbindung zu ermöglichen.

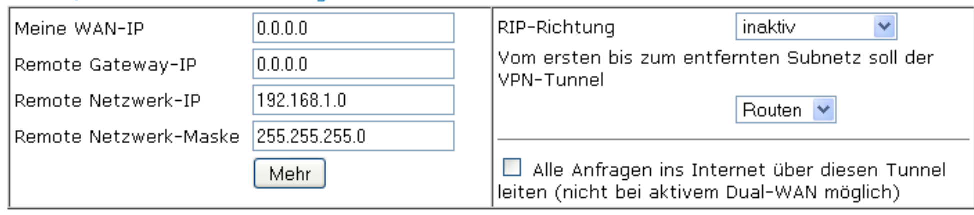
   Bei Auswahl eines ***IPSec-basierten*** Dienstes können Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Einwahlverbindung angeben. Ansonsten werden die obigen **IPSec Grundeinstellungen** verwendet.



Bei Auswahl eines ***PPP-basierten Dienstes*** müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort und VJ-Komprimierung für diese Einwahlverbindung angeben.

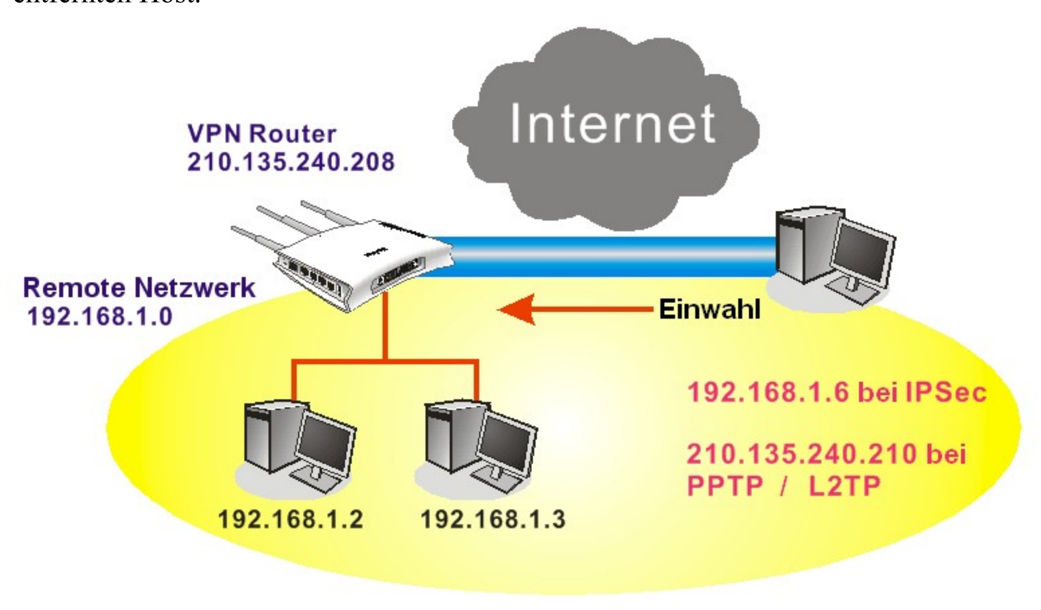


7. Schließlich konfigurieren Sie die entfernte Netzwerk-IP/das entfernte Subnetz in **TCP/IP-Netzwerkeinstellungen** so, dass der Router B die an Router A im entfernten Netzwerk bestimmten Pakete über die VPN-Verbindung übertragen kann.



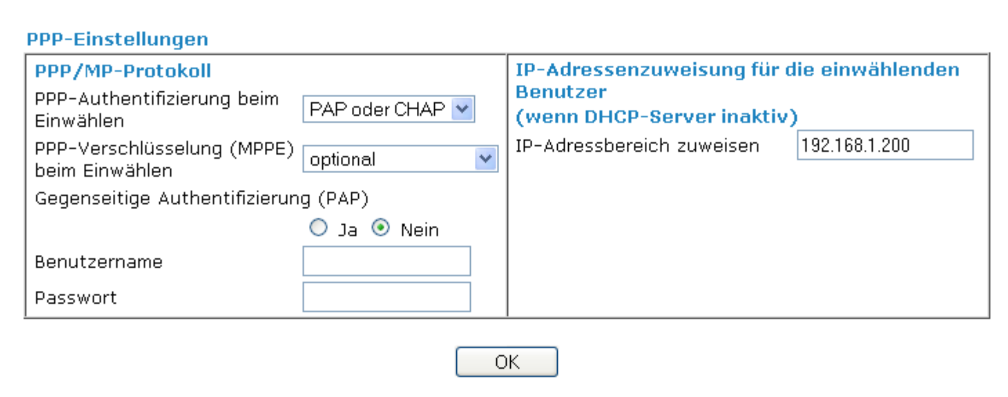
5.2 Einwahlverbindung zwischen externem Teleworker und Zentrale einrichten

Ein anderes verbreitetes Szenario: Ein Teleworker möchte eine sichere Verbindung zum Unternehmensnetzwerk aufbauen. Um die abgebildete Netzwerkstruktur einzurichten, erstellen Sie ein Fernbenutzerprofil und installieren einen Smart VPN Client auf dem entfernten Host.



Einstellungen auf dem VPN-Router im Unternehmensbüro:

1. Gehen Sie zu **VPN und externe Einwahl**, wählen Sie **Einwahlmöglichkeiten**, um den erforderlichen VPN-Dienst zu ermöglichen, und klicken Sie auf **OK**.
2. Um PPP-basierte Dienste wie PPTP oder L2TP zu verwenden, konfigurieren Sie die allgemeinen Einstellungen unter **PPP-Einstellungen**.



Um IPSec-basierte Dienste wie IPSec oder L2TP mit IPSec zu verwenden, konfigurieren Sie die Einstellungen in **IKE/IPSec-Grundeinstellungen**, z.B. den Pre-Shared Key, den beide Seiten kennen.

VPN und externe Einwahl >> IPSec Grundeinstellungen

IKE/IPSec Grundeinstellungen

Einstellungen für die Einwahl in diesen Router von außen (LAN-zu-LAN).

IKE-Authentifizierungsmethode

Pre-Shared Key ●●●●●●●●●●●

Pre-Shared Key bestätigen ●●●●●●●●●●●

IPSec-Sicherheitsmethode

☑ Mittel (AH)

Daten werden authentifiziert, aber nicht verschlüsselt.

Hoch (ESP) ☑ DES ☑ 3DES ☑ AES

Daten werden sowohl authentifiziert als auch verschlüsselt.

OK | Abbrechen

3. Gehen Sie zu **Externe Benutzer**. Klicken Sie auf eine der Indexnummern, um ein Profil zu bearbeiten.

4. Konfigurieren Sie die **Einstellungen zum Einwählen** wie unten angezeigt, um den entfernten Benutzer die Einwahl zum Aufbau einer VPN-Verbindung zu ermöglichen.

   Bei Auswahl eines ***IPSec-basierten*** Dienstes können Sie außerdem die IP-Adresse des entfernten Peers, die IKE-Authentifizierungsmethode und die IPSec-Verschlüsselungsmethode für diese Einwahlverbindung angeben. Ansonsten werden die obigen **IPSec Grundeinstellungen** verwendet.

VPN und externe Einwahl >> Externe Benutzer

Index-Nr. 1

Benutzerkonto und Authentifizierung

☐ aktiv

Max. Leerlaufzeit 300 Sekunden

Einwahl zulassen über

☐ PPTP

☑ IPSec

☐ L2TP mit IPSec ohne

☐ Fernzugriff definieren

IP oder ISDN-Nummer von entferntem Benutzer

oder Peer-ID

NetBIOS-Name durchlassen ◉ ja ○ nein

Benutzername ???

Passwort

IKE-Authentifizierungsmethode

☑ Pre-Shared Key

IKE Pre-Shared Key

☐ Digitale Signatur (X.509)

ohne

IPSec-Sicherheitsmethode

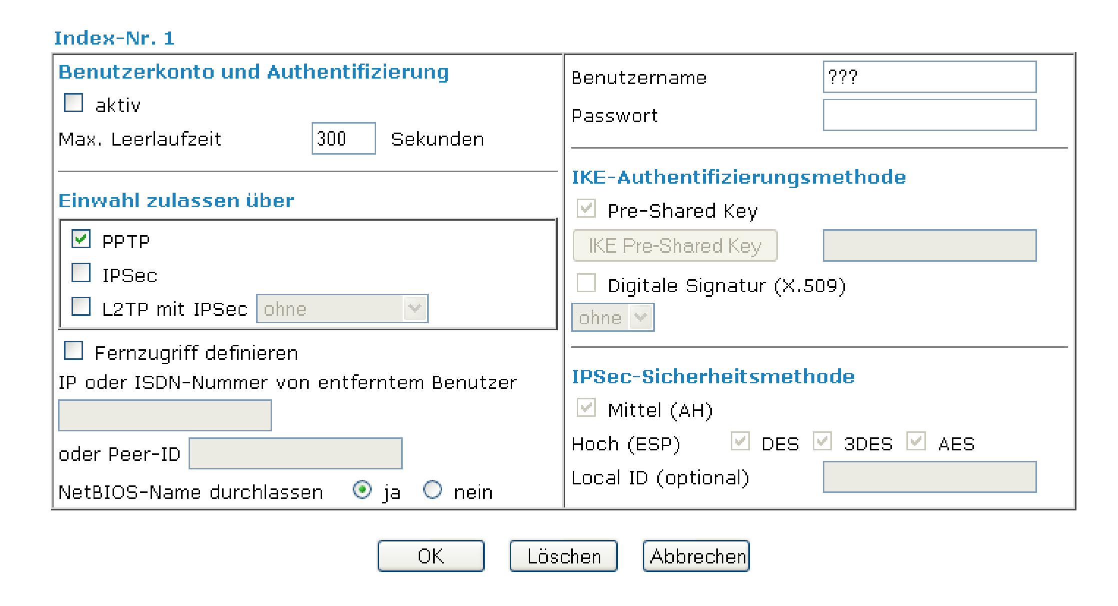
☑ Mittel (AH)

Hoch (ESP) ☑ DES ☑ 3DES ☑ AES

Local ID (optional)

OK | Löschen | Abbrechen

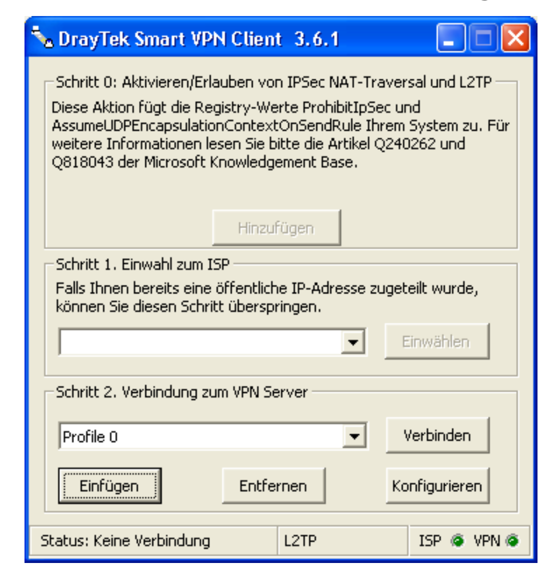
Bei Auswahl eines ***PPP-basierten*** Dienstes müssen Sie außerdem die IP-Adresse des entfernten Peers, den Benutzernamen, das Passwort und VJ-Komprimierung für diese Einwahlverbindung angeben.



Einstellungen auf dem entfernten Host:

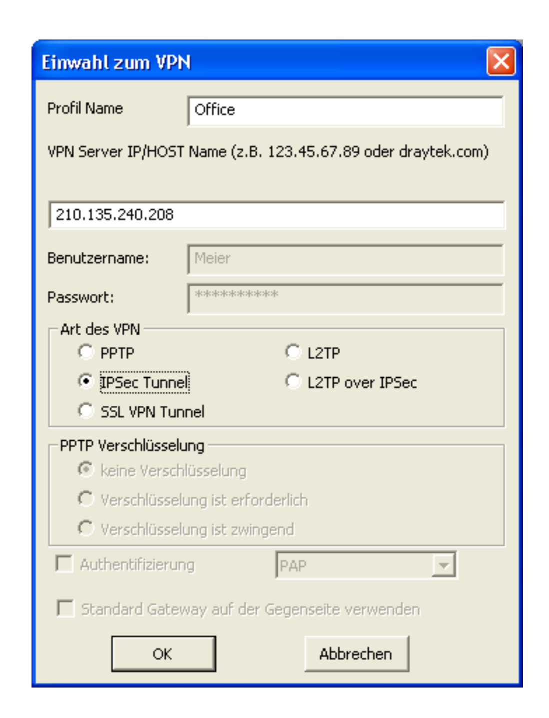
1. In Win98/ME können Sie "DFÜ-Netzwerk" verwenden, um einen PPTP-Tunnel zum Vigor-Router aufzubauen. In Win2000/XP verwenden Sie bitte die "Netzwerk- und Internetverbindungen" oder das kostenlose Programm "Smart VPN Client", um einen PPTP, L2TP bzw. L2TP über IPSec Tunnel aufzubauen. Dieses Programm kann von der beigefügten CD-ROM installiert werden oder von www.draytek.de heruntergeladen werden. Führen Sie die Installation gemäß den Anweisungen durch.

2. Nach erfolgreicher Installation sollten Sie bei erstmaliger Benutzung das **Profil 0.** einstellen. Klicken Sie dann auf **Konfigurieren**.

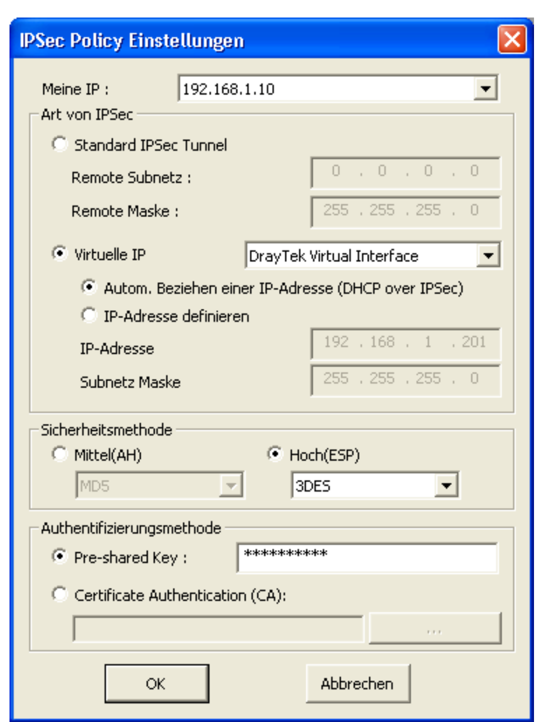


3. Im nächsten Schritt (**Einwahl zum VPN**) geben Sie die Informationen zur Einwahl auf den Server an.

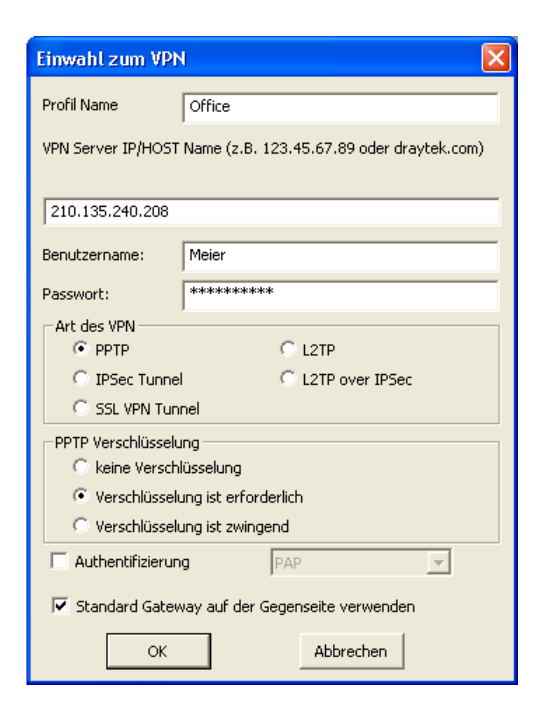
   Falls ein IPSec-basierter Dienst wie unten gezeigt gewählt wird …



... können Sie die Methode für die Zuweisung der IP, die Verschlüsselungsmethode und die Authentifizierungsmethode wählen. Bei Auswahl von Pre-Shared Key sollte dieser mit dem auf dem VPN-Router Konfigurierten übereinstimmen.



Bei Auswahl eines PPP-basierten Dienstes müssen Sie außerdem die IP-Adresse des entfernten VPN-Servers, den Benutzernamen, das Passwort und die Verschlüsselungsmethode angeben. Der Benutzername und das Passwort sollten den auf dem VPN-Router konfigurierten Daten entsprechen. "Use default gateway on remote network" bedeutet, dass alle Pakete des entfernten Hosts zum VPN-Server und von dort ins Internet gesendet werden. So erscheint es, als würde sich der entfernte Host im Unternehmensnetzwerk befinden.

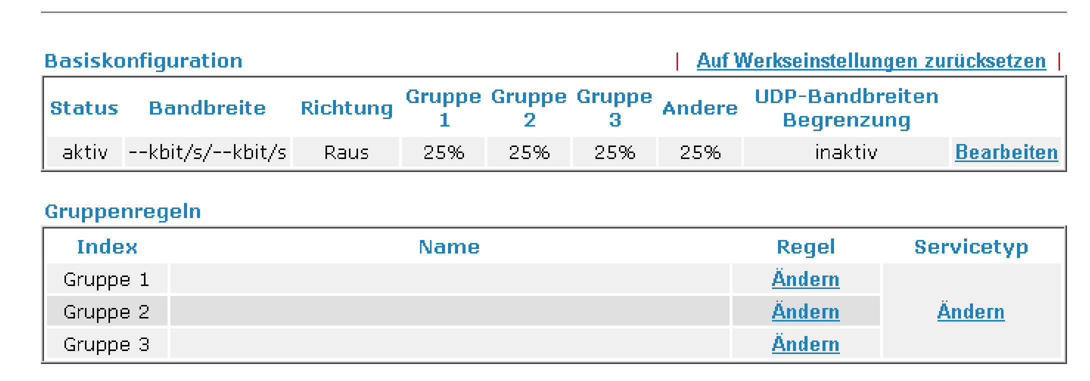


4. Klicken Sie auf **Connect**, um die Verbindung aufzubauen. Wenn die Verbindung erfolgreich ist, wird unten rechts eine grüne Lampe angezeigt.

5.3 Beispiel für QoS-Einstellungen

Nehmen wir an, ein Teleworker arbeitet teilweise zu Hause, um seine Kinder beaufsichtigen zu können. Während seiner Arbeitszeit verwendet er seinen Vigor-Router zuhause, um sich über HTTPS oder VPN mit dem Server in der Zentrale zu verbinden und so Zugriff auf seine E-Mails und auf die interne Datenbank zu erlangen. Gleichzeitig verwenden die Kinder im Zimmer nebenan Skype.

1. Gehen Sie zu **Bandbreitenmanagement>>Quality of Service.**



Bandbreitenmanagement >> Quality of Service

Basiskonfiguration | Auf Werkseinstellungen zurücksetzen |

Status	Bandbreite	Richtung	Gruppe 1	Gruppe 2	Gruppe 3	Andere	UDP-Bandbreiten Begrenzung	
aktiv	--kbit/s/--kbit/s	Raus	25%	25%	25%	25%	inaktiv	Bearbeiten

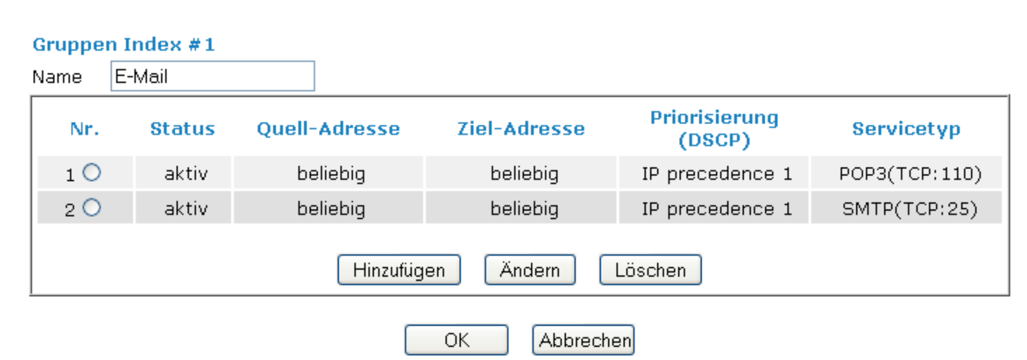
Gruppenregeln

Index	Name	Regel	Servicetyp
Gruppe 1		Ändern	Ändern
Gruppe 2		Ändern	
Gruppe 3		Ändern	

2. Klicken Sie auf **Bearbeiten**. Sorgen Sie dafür, dass **aktiv** in der rechten Ecke markiert ist. Wählen Sie unter **Richtung Beide**.

Basiskonfiguration
aktiv Beide
Rein
Raus
Beide

3. Kehren Sie zur vorherigen Seite zurück. Geben Sie den Namen der Indexklasse 1 ein, indem Sie auf **Bearbeiten** klicken. Geben Sie für Klasse 1 den Namen "**E-Mail**" ein.



Bandbreitenmanagement >> Quality of Service

Gruppen Index #1

Name E-Mail

Nr.	Status	Quell-Adresse	Ziel-Adresse	Priorisierung (DSCP)	Servicetyp
1	aktiv	beliebig	beliebig	IP precedence 1	POP3(TCP:110)
2	aktiv	beliebig	beliebig	IP precedence 1	SMTP(TCP:25)

Hinzufügen Ändern Löschen

OK Abbrechen

4. In diesem Index kann der Benutzer die reservierte Bandbreite (z.B. 25%) für **E-Mail** über die Protokolle POP3 und SMTP bestimmen.

Bandbreitenmanagement >> Quality of Service

Basiskonfiguration

☑ aktiv Raus

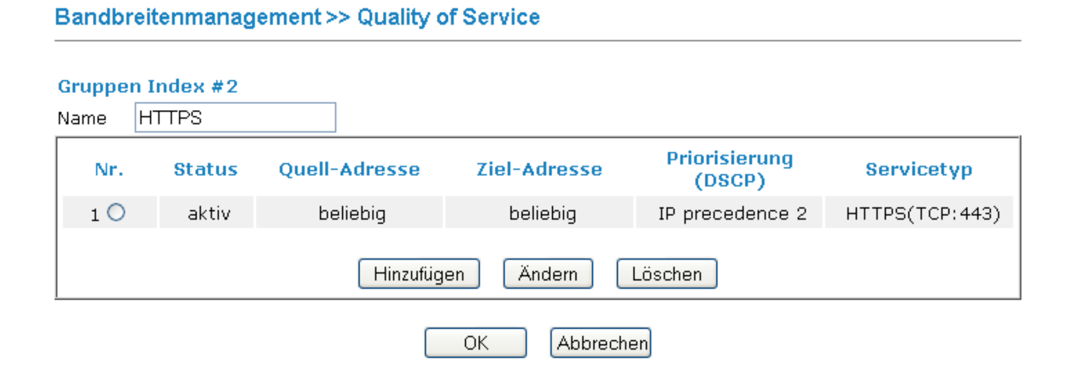
Index	Gruppenname	Reservierte Bandbreite
Gruppe 1	E-Mail	25 %
Gruppe 2		25 %
Gruppe 3		25 %
	Andere	25 %

☐ UDP-Bandbreite begrenzen — Maximale Bandbreite für UDP 25 %

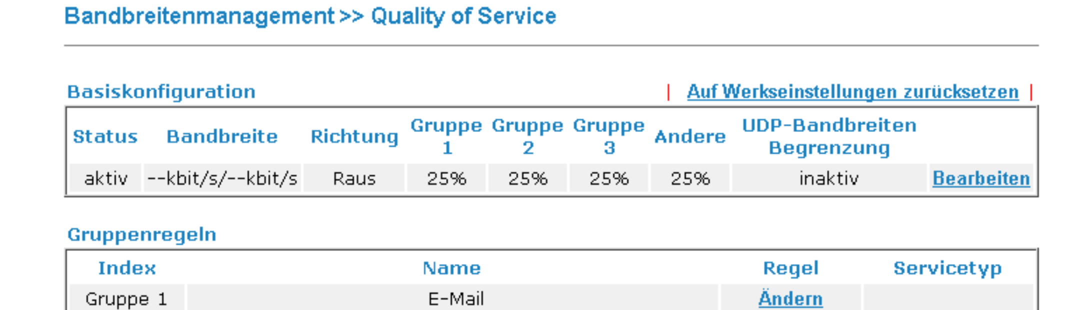
☐ ausgehende TCP-ACK-Pakete priorisieren — Online-Statistik

OK | Löschen | Abbrechen

5. Kehren Sie zur vorherigen Seite zurück. Geben Sie den Namen der Indexklasse 2 ein, indem Sie auf **Bearbeiten** klicken. In diesem Index kann der Benutzer die reservierte Bandbreite für **HTTPS** bestimmen. Klicken Sie auf **OK**.



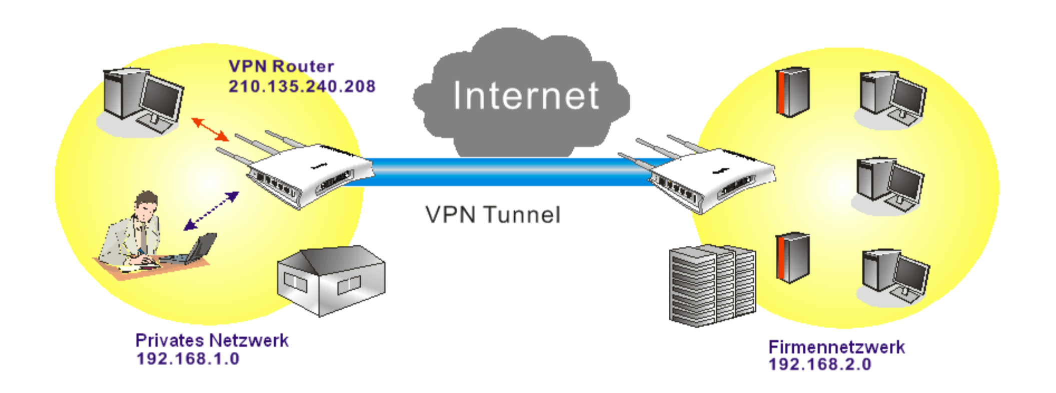
6. Klicken Sie auf **Bearbeiten**, um die reservierte Bandbreite zu setzen.





7. Klicken Sie unten auf **UDP-Bandbreite begrenzen**, um zu vermeiden, dass übermäßiger UDP-Verkehr VoIP oder andere Anwendungen beeinträchtigt. Klicken Sie auf **OK**.

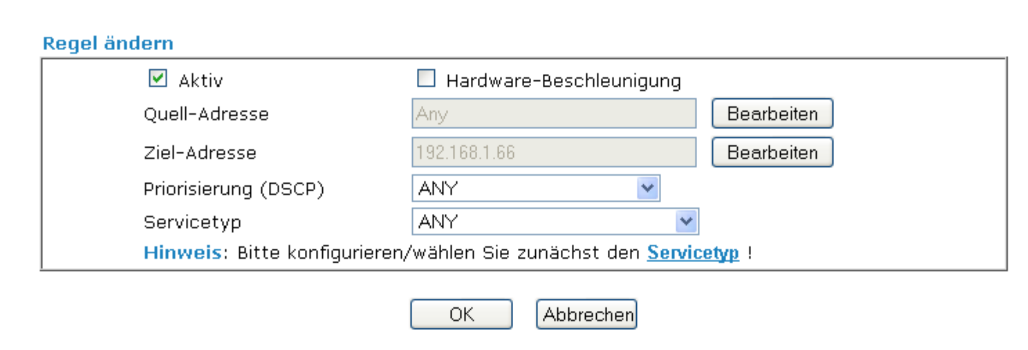
8. Falls sich der Teleworker über einen Host-zu-Host-Tunnel mit der Zentrale verbunden hat (siehe detaillierte Anweisungen in Kapitel 3 "VPN"), kann er hierfür einen Index einrichten. Geben Sie die Bezeichnung der Klasse von Index 3 an. In diesem Index kann die reservierte Bandbreite für einen VPN-Tunnel bestimmt werden.



9. Klicken Sie auf **Hinzufügen**

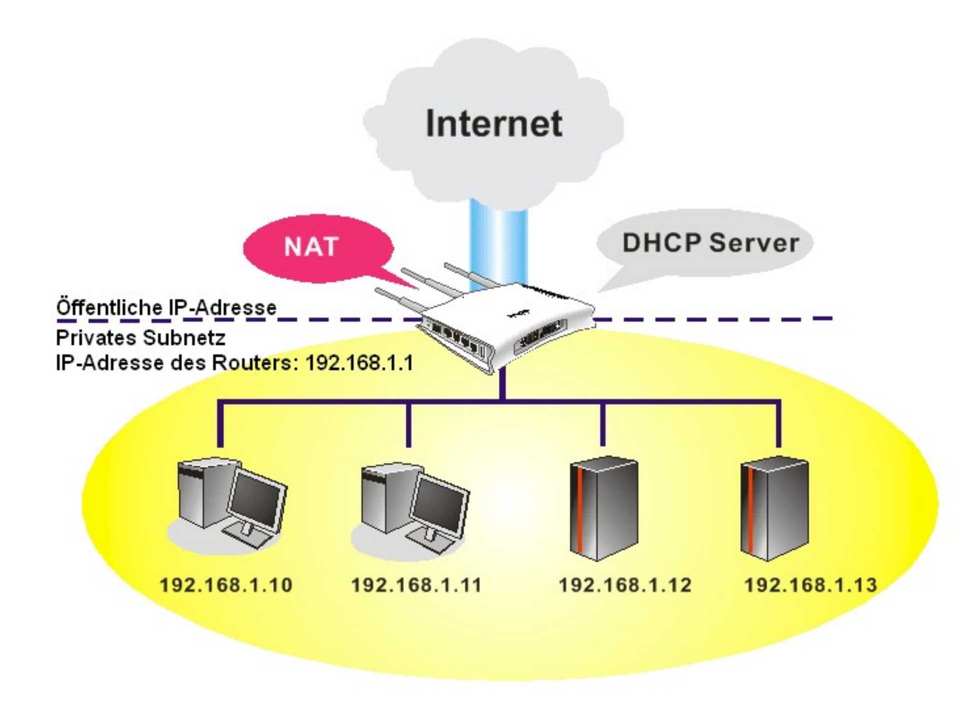


10. Markieren Sie zunächst **Aktiv** und klicken Sie dann auf **Bearbeiten** neben **Quell-Adresse**, um die Subnetzadresse des Teleworkers einzustellen. Klicken Sie auf **Bearbeiten** neben **Ziel-Adresse**, um die IP-Adresse der Zentrale einzugeben. Lassen Sie alle anderen Felder, wie sie sind, und klicken Sie auf **OK**.



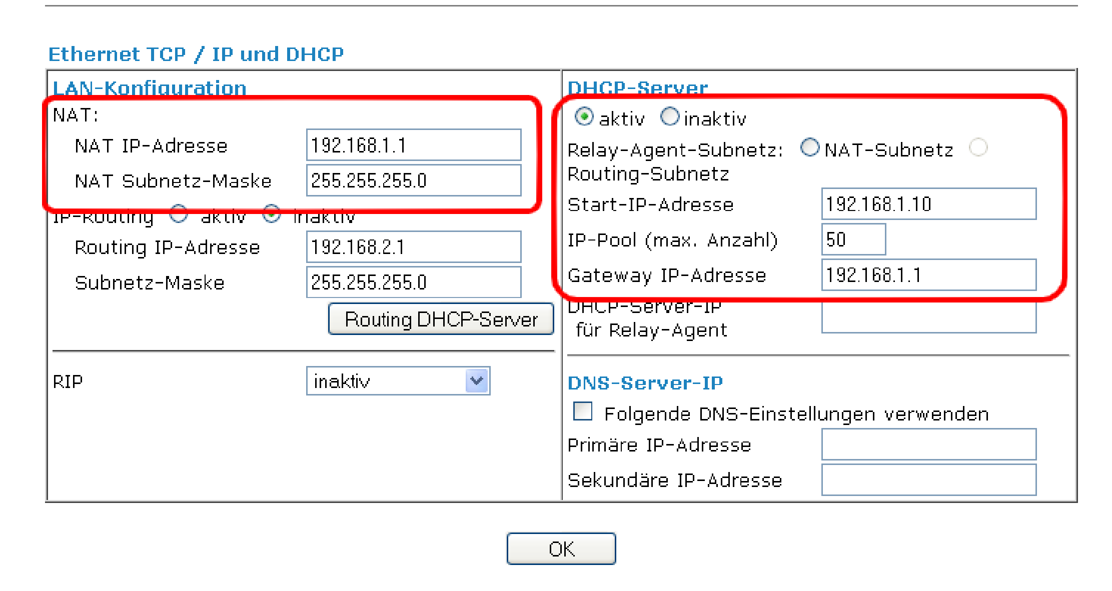
5.4 LAN – Einrichtung mit NAT

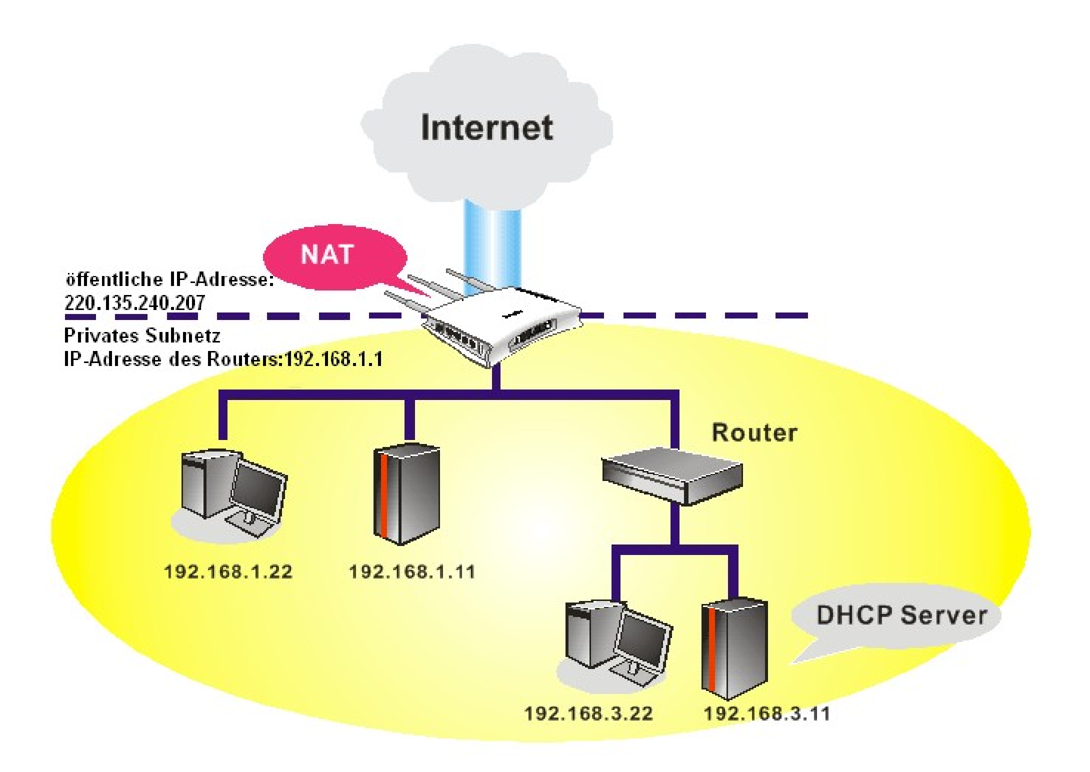
Die folgende Abbildung zeigt die Standardeinstellungen und ein Einsatzbeispiel. Die Standardwerte für private IP-Adresse/Subnetz-Maske sind 192.168.1.1/255.255.255.0. Der eingebaute DHCP-Server ist so konfiguriert, dass er jedem NAT-Host eine IP-Adresse zwischen 192.168.1.10 und 192.168.1.50 zuweist.



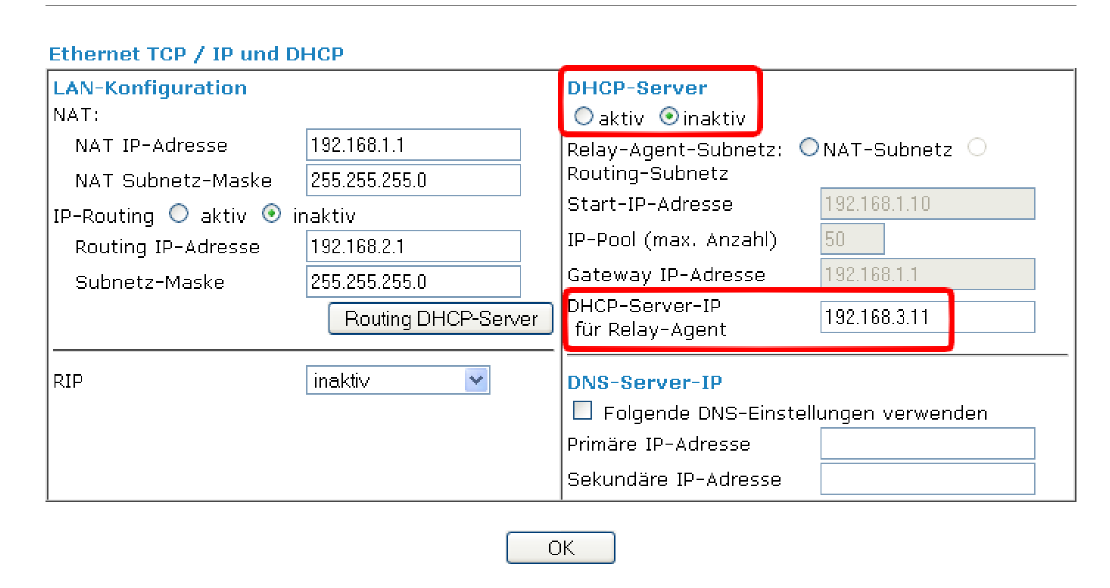
Sie können die rot eingerahmten Einstellungen den Anforderungen Ihrer NAT-Nutzung anpassen.

Um im Netzwerk einen anderen DHCP-Server als den eingebauten DHCP-Server des Vigor-Routers zu verwenden, müssen Sie die Einstellungen wie unten gezeigt ändern.





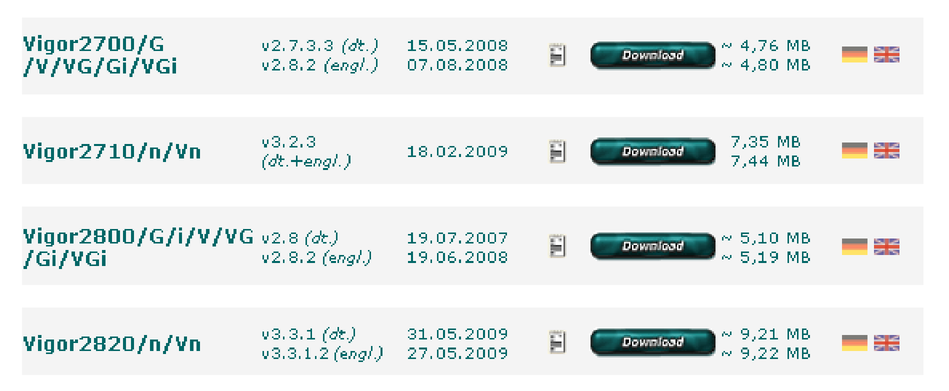
Sie können die rot eingerahmten Einstellungen den Anforderungen Ihrer NAT-Nutzung anpassen.



5.5 Firmware des Routers aktualisieren

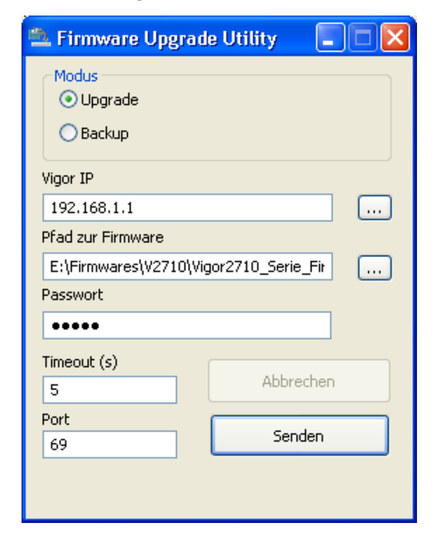
Um Ihre Router-Firmware zu aktualisieren müssen Sie das **Firmware Upgrade Utility** installieren, welches Sie von der beigefügten CD oder über unsere Homepage www.draytek.de erhalten.

1. Gehen Sie zu **www.draytek.de**, um die neueste Firmware für Ihren Router zu finden.
2. Gehen Sie zu **Downloads** >> **Firmware**. Suchen Sie nach der Modellbezeichnung des Routers und klicken Sie auf den Firmware-Link.



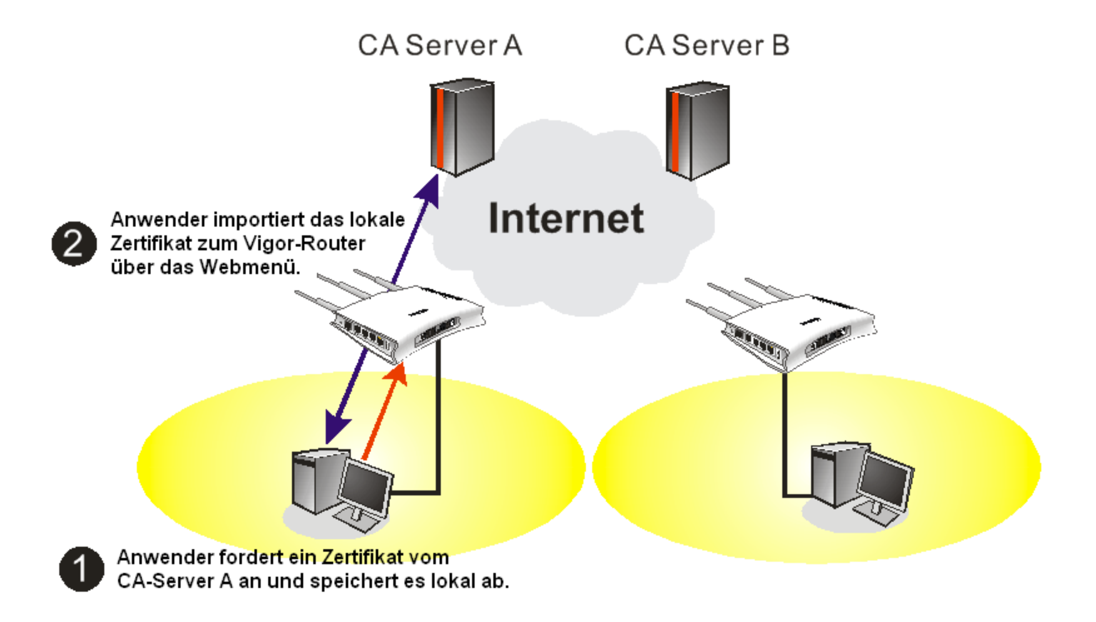
Modell	Version	Datum	Download	Größe
Vigor2700/G /V/VG/Gi/VGi	v2.7.3.3 (dt.) v2.8.2 (engl.)	15.05.2008 07.08.2008	Download	~ 4,76 MB ~ 4,80 MB
Vigor2710/n/Vn	v3.2.3 (dt.+engl.)	18.02.2009	Download	7,35 MB 7,44 MB
Vigor2800/G/i/V/VG /Gi/VGi	v2.8 (dt.) v2.8.2 (engl.)	19.07.2007 19.06.2008	Download	~ 5,10 MB ~ 5,19 MB
Vigor2820/n/Vn	v3.3.1 (dt.) v3.3.1.2 (engl.)	31.05.2009 27.05.2009	Download	~ 9,21 MB ~ 9,22 MB

3. Wählen Sie die Datei, die Ihrem Betriebssystem entspricht, und klicken Sie auf den entsprechenden Link, um die korrekte Firmware herunterzuladen (ZIP-Datei).
4. Dekomprimieren Sie die ZIP-Datei.
5. Starten Sie das Firmware Upgrade Utility.
6. Geben Sie Ihre Router-IP ein, normalerweise **192.168.1.1**.
7. Klicken Sie auf die Taste rechts neben dem Feld, das die Firmware-Datei enthält. Wählen Sie die Datei, die Sie von der Web-Site des Herstellers heruntergeladen haben. Sie werden zwei Dateien mit unterschiedlichen Erweiterungen sehen, **xxxx.all** (erhält die benutzerspezifischen Einstellungen) **u**nd **xxxx.rst** (setzt alle benutzerspezifischen Einstellungen auf die Werkseinstellungen zurück). Wählen Sie die benötigte Datei.



8. Klicken Sie auf **Senden**.
9. Die erfolgreiche Aktualisierung wird mit einer Nachricht bestätigt.

5.6 Zertifikat von einem CA-Server oder Windows CA-Server anfordern



1. Gehen Sie zur **Zertifikatsverwaltung** und wählen Sie **Lokales Zertifikat**.

Zertifikatsverwaltung >> lokales Zertifikat

X.509 lokales Zertifikat konfigurieren

Name	Subjekt	Status	Ändern
lokal		Requesting	Ansicht Löschen

Erstellen Importieren Aktualisieren

lokale X.509 Zertifikatsanfrage

2. Klicken Sie auf **Erstellen**, um ein Zertifikat zu erstellen. Geben Sie die Daten ein, die zur Erstellung eines Zertifikats erforderlich sind.

Zertifikatsverwaltung >> lokales Zertifikat

Zertifikat erstellen

Alternativer Name

Typ IP-Adresse

IP

Name

Land (C)

Bundesland (ST)

Ort (L)

Organisation (O)

Abteilung (OU)

Bezeichnung (CN)

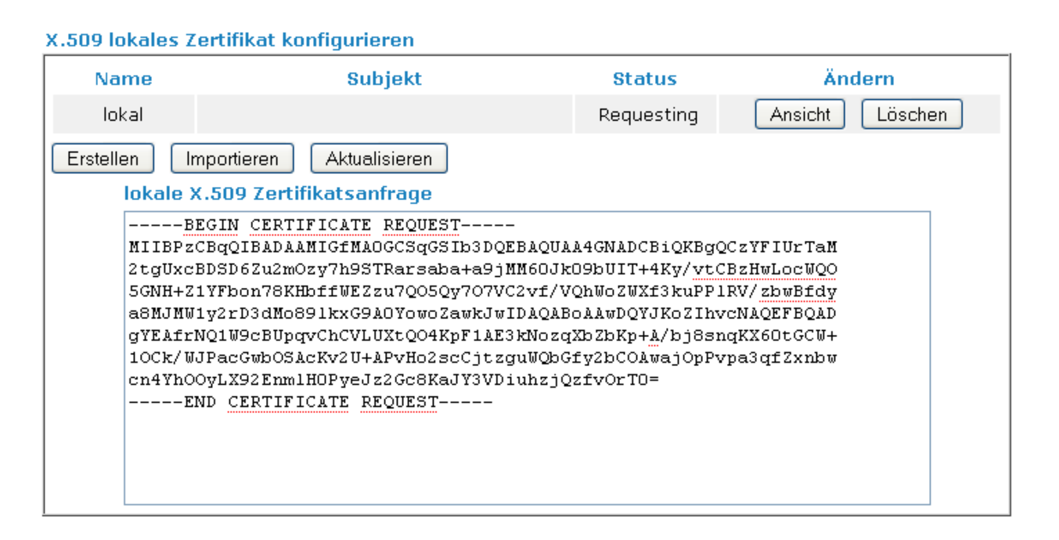
E-Mail (E)

Schlüsseltyp RSA

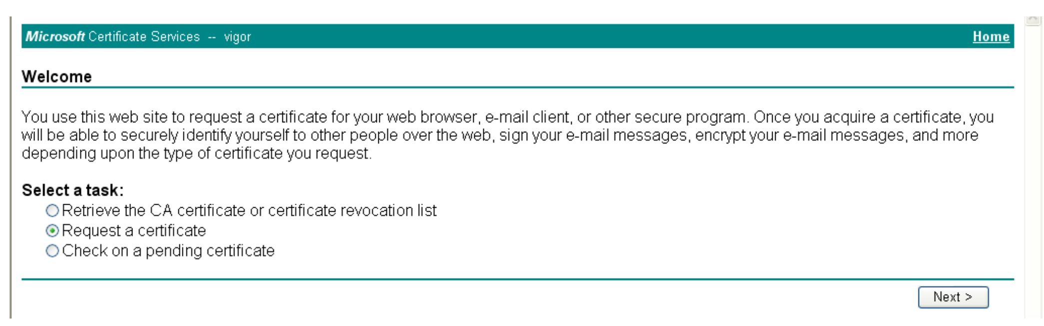
Schlüsselgröße 1024 bit

Erstellen

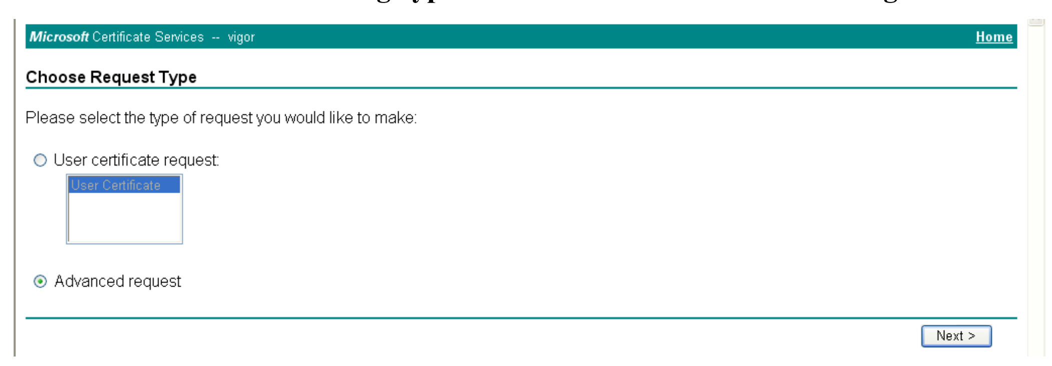
3. Kopieren und speichern Sie die lokale X.509 Zertifikatsanfrage als Textdatei und bewahren Sie sie für späteren Gebrauch auf.



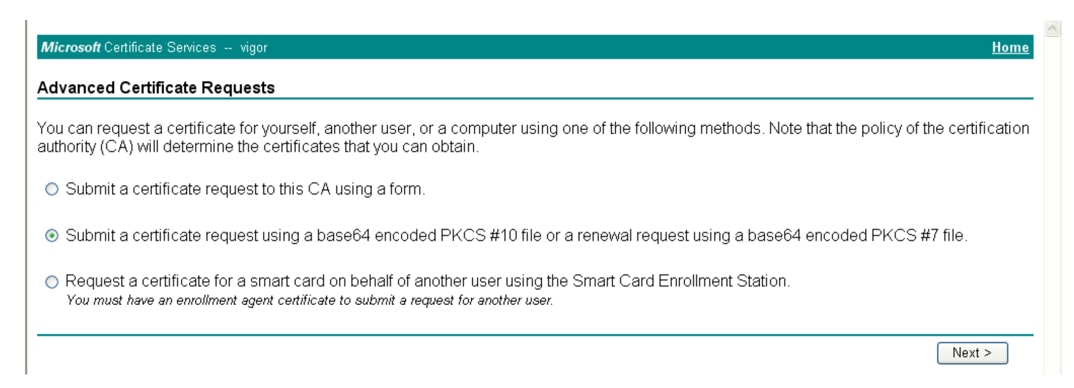
4. Verbinden Sie sich über den Web-Browser mit dem CA-Server. Folgen Sie den Anweisungen, um die Anfrage zu stellen. Das folgende Beispiel zeigt einen Windows 2000 CA-Server. Wählen Sie **Ein Zertifikat anfordern** und klicken Sie auf **Weiter**.



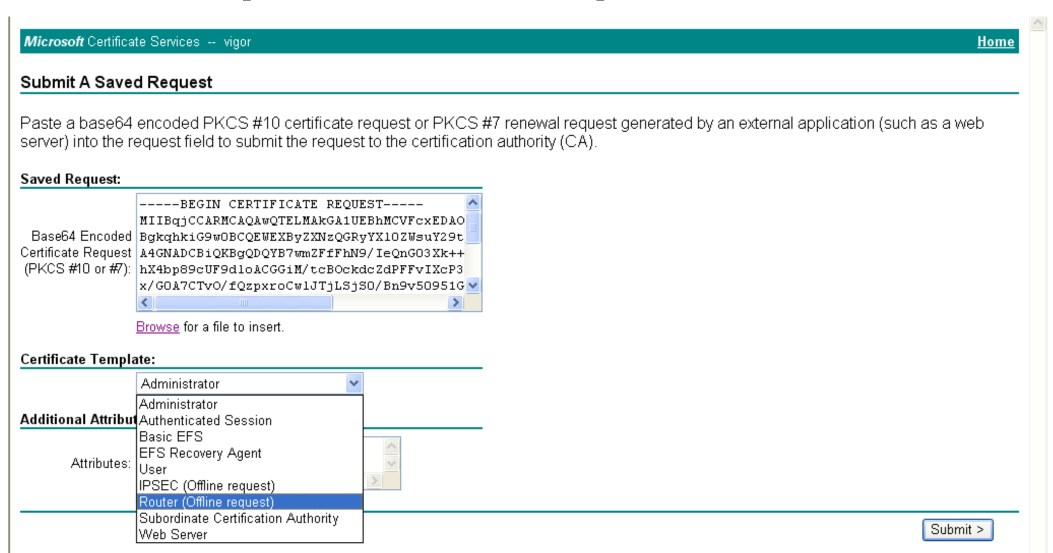
Klicken Sie unter **Anforderungstyp wählen** auf **Erweiterte Anforderung**.



Wählen Sie **Senden Sie eine Zertifikatsanforderung ein, die eine Base64-codierte PKCS10-Datei verwendet, oder eine Erneuerungsanforderung, die eine Base64-codierte PKCS7-Datei verwendet**.



Importieren Sie die lokale X.509 Zertifikatsanforderungsdatei. Wählen Sie unten **Router (Offline request)** oder **IPSec (Offline request)**.

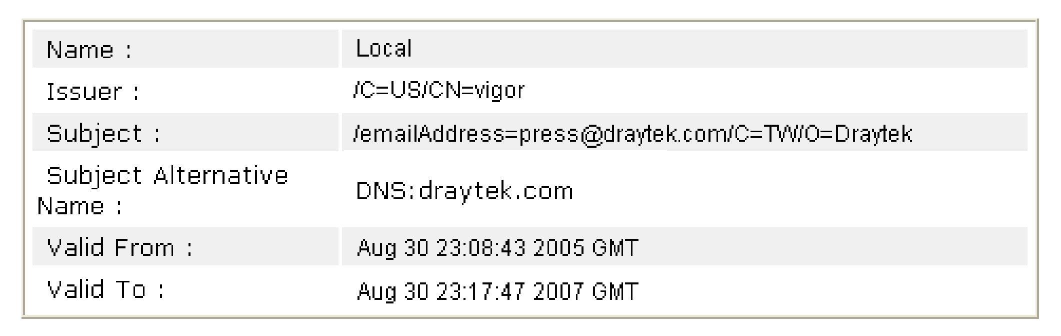


Nach Absenden der Anforderung stellt der Server ein Zertifikat aus. Wählen Sie **Base64-codiertes Zertifikat** und **Download des Zertifizierungsstellenzertifikats**. Speichern Sie das Zertifikat (.cer-Datei) ab.

5. Auf dem Vigor-Router gehen Sie zu **Lokales Zertifikat**. Klicken Sie auf **Importieren** und wählen Sie die entsprechende Datei, um das Zertifikat (.cer-Datei) auf dem Vigor-Router zu importieren. Klicken Sie nach Abschluss auf **Aktualisieren**; im Feld unten erscheint "BEGIN CERTIFICATE ...".

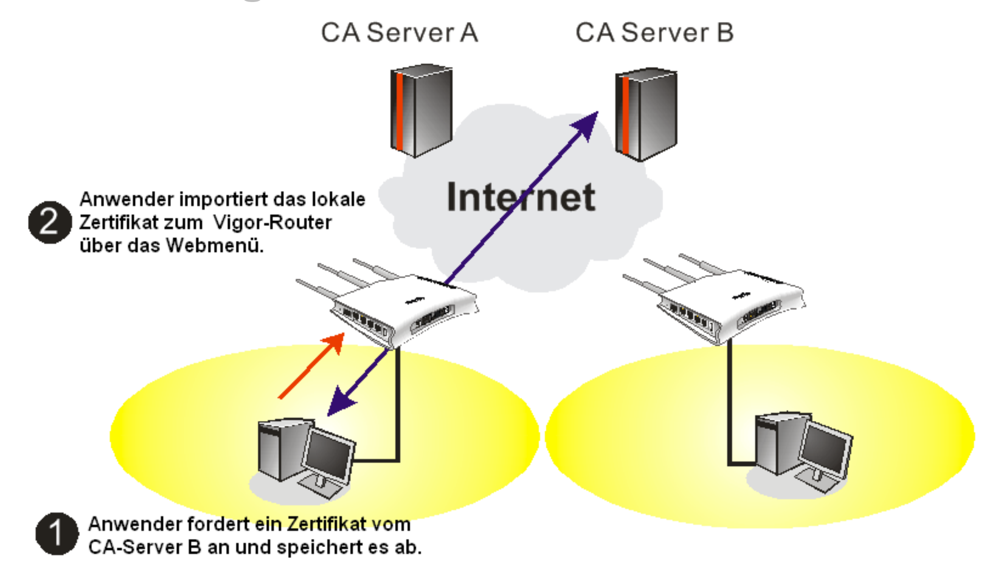


6. Sie können die Details des Zertifikats kontrollieren, indem Sie auf **Ansicht** klicken.

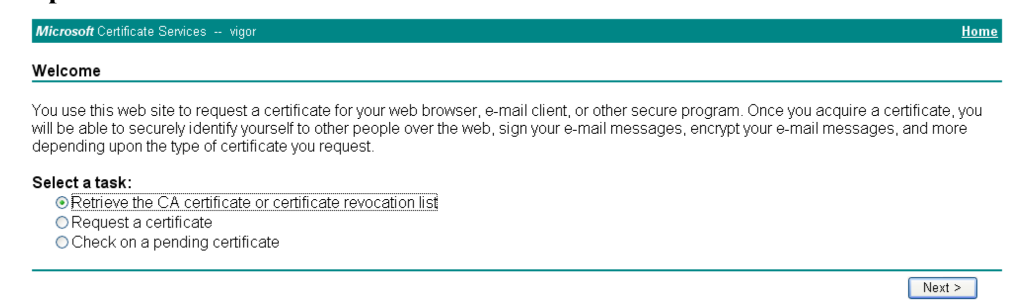


Name :	Local
Issuer :	/C=US/CN=vigor
Subject :	/emailAddress=press@draytek.com/C=TW/O=Draytek
Subject Alternative Name :	DNS:draytek.com
Valid From :	Aug 30 23:08:43 2005 GMT
Valid To :	Aug 30 23:17:47 2007 GMT

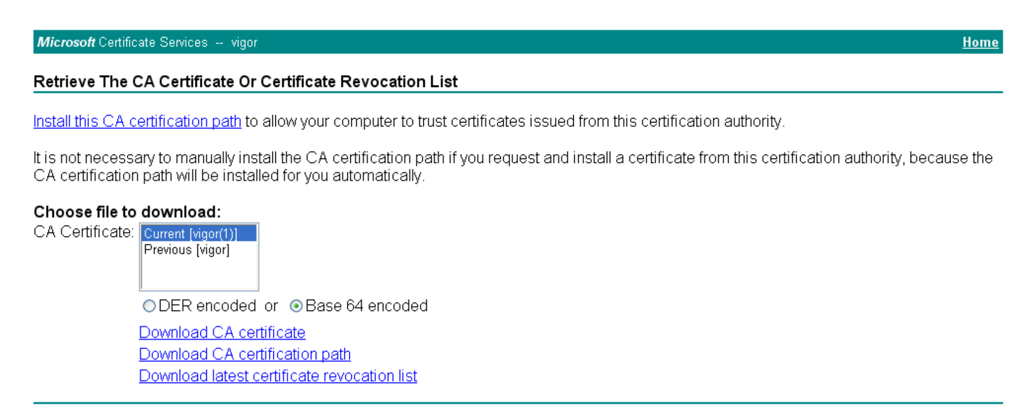
5.7 CA-Zertifikat von Windows CA-Server anfordern und als vertrauenswürdiges Zertifikat setzen



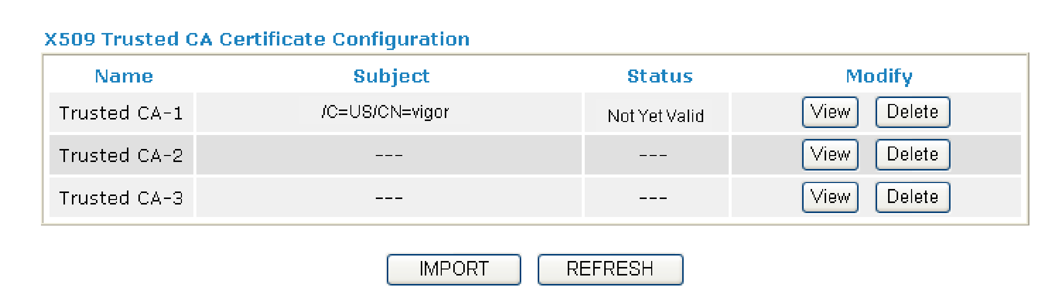
1. Benutzen Sie den Web-Browser, um sich mit dem CA-Server zu verbinden, von dem Sie ein CA-Zertifikat herunterladen möchten. Klicken Sie auf **Download eines Zertifizierungstellenzertifikats, einer Zertifikatkette oder einer Sperrliste**.



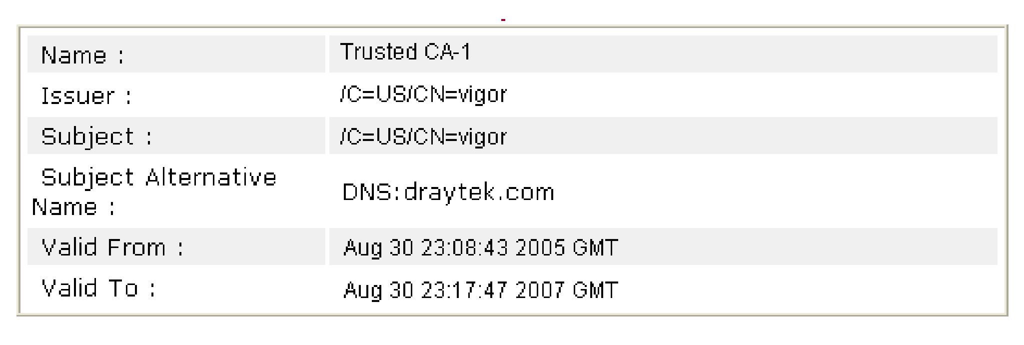
2. Unter **Datei zum Downloaden auswählen** klicken Sie auf das CA-Zertifikat **Current** und auf **Base64-codiert** und dann auf **Download des Zertifizierungsstellenzertifikats**, um die .cer-Datei zu speichern.



3. Auf dem Vigor-Router gehen Sie zu **Vertrauenswürdiges CA-Zertifikat**. Klicken Sie auf **Importieren** und wählen Sie die entsprechende Datei, um das Zertifikat (.cer-Datei) auf dem Vigor-Router zu importieren. Klicken Sie nach Abschluss auf **Aktualisieren**, damit die Information wie folgt angezeigt wird.



4. Sie können die Details des Zertifikats kontrollieren, indem Sie auf **Ansicht** klicken.



Hinweis: Bevor Sie das Zertifikat konfigurieren, stellen Sie bitte unter **Systemmanagement >> Zeit und Datum** die aktuelle Zeit des Routers ein.

6 Fehlersuche

Dieser Abschnitt hilft Ihnen, Probleme zu lösen, falls Sie nach Installation des Routers und Abschluss der Web-Konfiguration keinen Zugang zum Internet haben. Bitte folgen Sie den Anweisungen, um Ihre Basiskonfiguration schrittweise zu überprüfen.

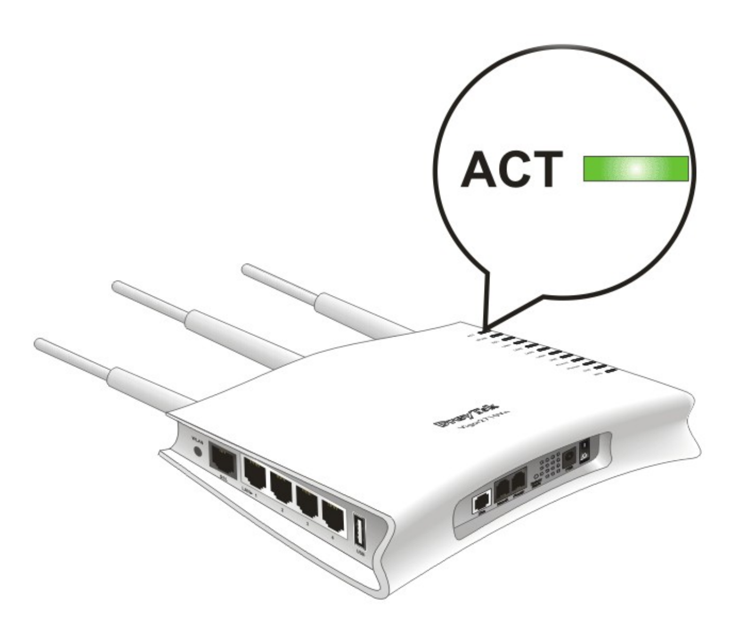
- Kontrollieren, ob der Hardware-Status in Ordnung ist.
- Kontrollieren, ob die Netzwerkverbindungseinstellungen auf Ihrem Rechner in Ordnung sind.
- Den Router von Ihrem Rechner anpingen.
- Kontrollieren, ob die ISP-Einstellungen in Ordnung sind.
- Falls erforderlich, auf Werkseinstellungen zurücksetzen.

Falls der Router immer noch nicht ordnungsgemäß funktioniert, obwohl Sie alle beschriebenen Schritte durchgeführt haben, ist es an der Zeit, sich für weitere Unterstützung an Ihren Händler zu wenden.

6.1 Hardwarestatus überprüfen

Befolgen Sie die folgenden Schritte, um den Hardware-Status zu kontrollieren:

1. Überprüfen Sie die Stromversorgung und die LAN-Kabelverbindungen. Sehen Sie zu Einzelheiten Abschnitt **1.3** "**Hardwareinstallation**".
2. Schalten Sie den Router ein. Die **ACT LED** muss einmal pro Sekunde blinken, und die **LAN LED** muss leuchten.



3. Falls dies nicht der Fall ist, ist der Hardwarestatus nicht in Ordnung. Gehen Sie zurück zu **1.3** "**Hardwareinstallation**", um die Hardwareinstallation nochmals auszuführen. Danach versuchen Sie es erneut.

6.2 Netzwerkeinstellungen am PC kontrollieren

Manchmal funktionieren Links aufgrund falscher Netzwerkverbindungseinstellungen nicht. Falls ein Link trotz Anwendung der Anweisungen im obigen Abschnitt immer noch nicht funktioniert, folgen Sie bitten den folgenden Anweisungen, um zu kontrollieren, ob die Netzwerkverbindungseinstellungen in Ordnung sind.

Für Windows

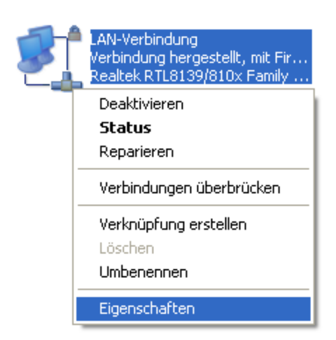


Das Beispiel verwendet Windows XP. Sofern die Schritte für andere Betriebssysteme nicht ähnlich sind, sehen Sie bitte die Hinweise unter **www.draytek.de**.

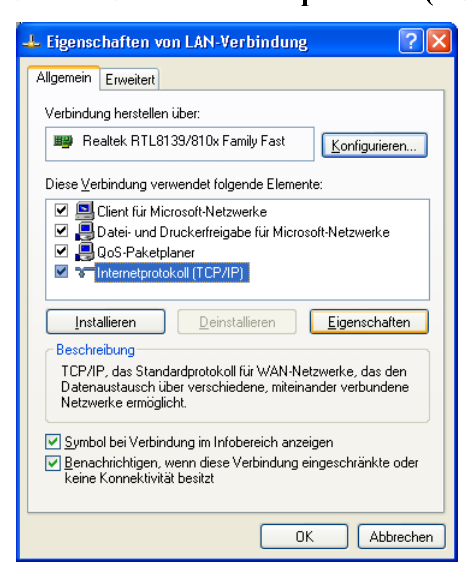
1. Gehen Sie zur **Systemsteuerung** und klicken Sie **Netzwerkverbindungen** doppelt an.



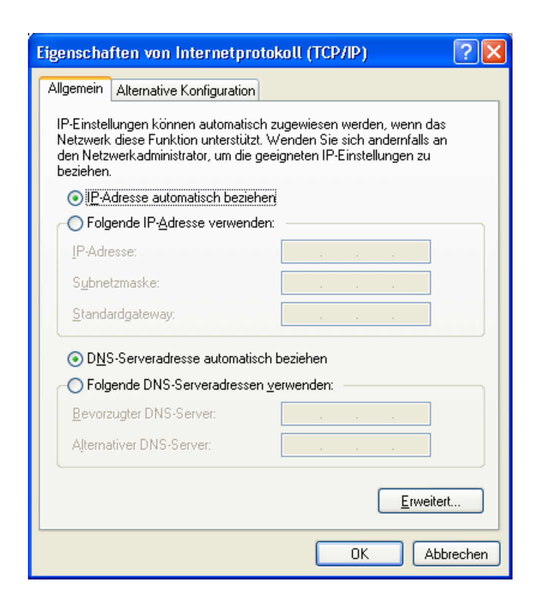
2. Klicken Sie die **LAN-Verbindung** mit der rechten Maustaste an und klicken Sie auf **Eigenschaften**.



3. Wählen Sie das **Internetprotokoll (TCP/IP)** und klicken Sie auf **Eigenschaften**.

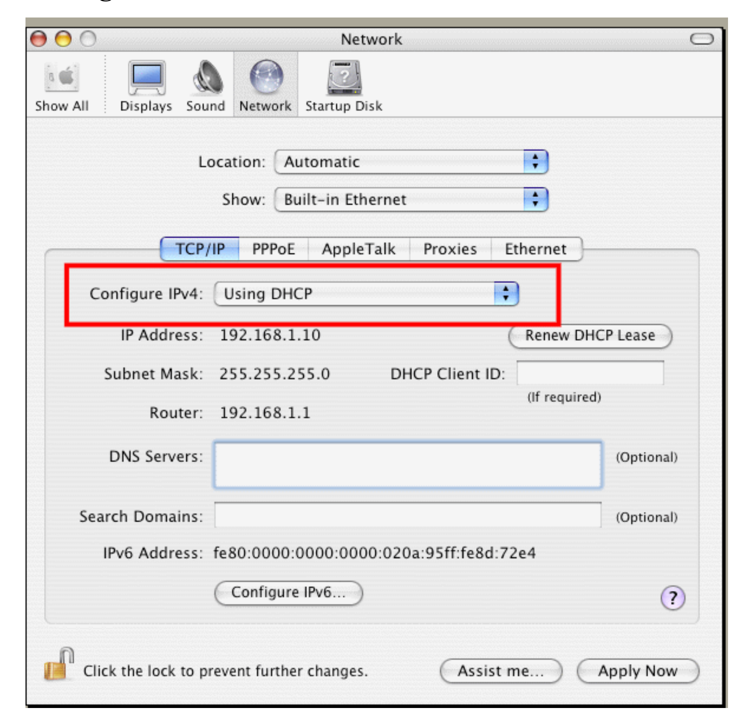


4. Wählen Sie **IP-Adresse automatisch beziehen** und **DNS-Serveradresse automatisch beziehen**.



Für MacOS

1. Klicken Sie in MacOS doppelt auf den Arbeitsbereich.
2. Öffnen Sie den Ordner **Programme** und wählen Sie **Netzwerk**.
3. Im Menü **Netzwerk** wählen Sie **DHCP** aus der Dropdown-Liste **IPv4 konfigurieren**.



6.3 Pingen des Routers von Ihrem PC aus

Die Standard-Gateway-IP-Adresse des Routers ist 192.168.1.1. Es mag notwendig sein, den Befehl "ping" zu verwenden, um den Verbindungsstatus des Routers zu kontrollieren. **Es ist wichtig, dass der Rechner eine Antwort von 192.168.1.1 erhält.** Falls dies nicht geschieht, überprüfen Sie bitte die IP-Adresse Ihres Rechners. Wir empfehlen, die Netzwerkverbindung so zu konfigurieren, dass die **IP automatisch bezogen** wird (siehe Abschnitt 4.2)

Befolgen Sie die folgenden Schritte, um den Router anzupingen.

Für Windows

1. Öffnen Sie die **Eingabeaufforderung** (unter **Start> Ausführen**).
2. Geben Sie **command** (Windows 95/98/ME) bzw. **cmd** (Windows NT/2000/XP) ein. Die DOS-Eingabeaufforderung erscheint.

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Dokumente und Einstellungen\Axel>ping 192.168.1.1

Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:

Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit<1ms TTL=255

Ping-Statistik für 192.168.1.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 0ms, Maximum = 0ms, Mittelwert = 0ms

C:\Dokumente und Einstellungen\Axel>
```

3. Geben Sie **ping 192.168.1.1** ein und drücken auf [Enter]. Falls der Link in Ordnung ist, erscheint die Zeile "**Reply from 192.168.1.1:bytes=32 time<1ms TTL=255**".
4. Falls diese Zeile nicht erscheint, kontrollieren Sie bitte die IP-Adresse Ihres Rechners.

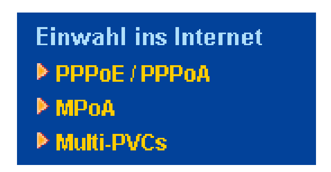
Für MacOS (Terminal)

1. Klicken Sie in MacOS doppelt auf den Arbeitsbereich.
2. Öffnen Sie den Ordner **Programme** und wählen Sie **Dienstprogramme**.
3. Klicken Sie **Terminal** doppelt an. Das Terminalfenster erscheint.
4. Geben Sie **ping 192.168.1.1** ein und drücken auf [Enter]. Falls der Link in Ordnung ist, erscheint die Zeile "**64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=xxxx ms**".

```
Terminal — bash — 80x24
Last login: Sat Jan  3 02:24:18 on ttyp1
Welcome to Darwin!
Vigor10:~ draytek$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=255 time=0.755 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=255 time=0.697 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=255 time=0.716 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=255 time=0.731 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=255 time=0.72 ms
^C
--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.697/0.723/0.755 ms
Vigor10:~ draytek$
```

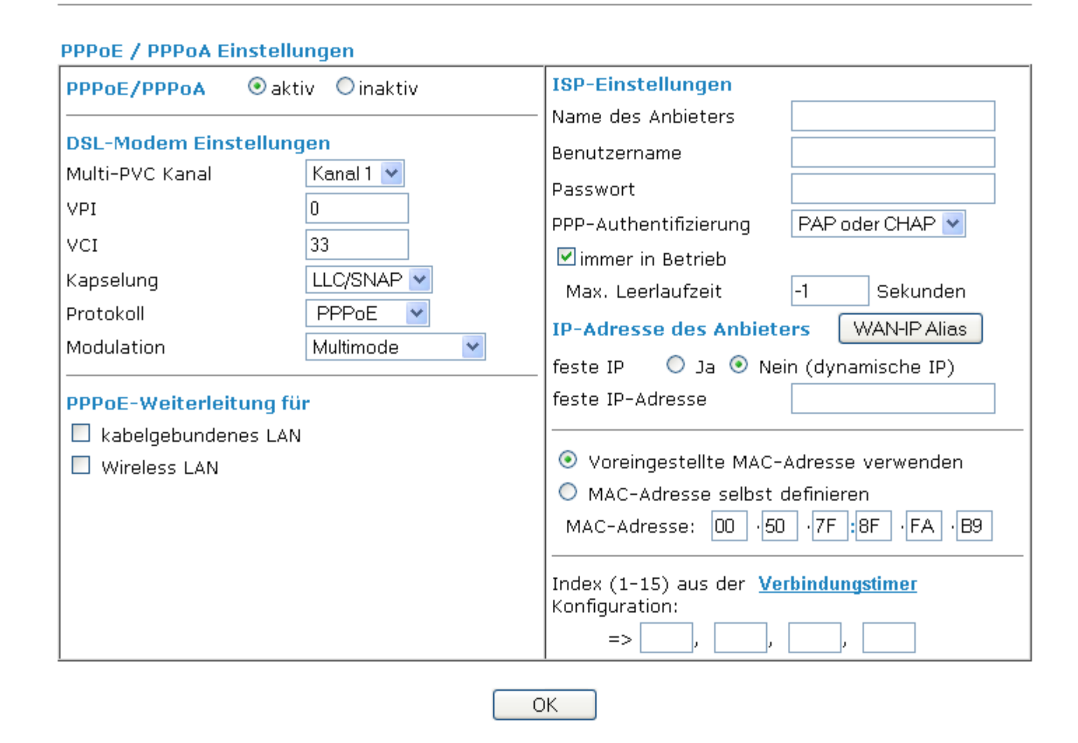
6.4 Prüfen der ISP-Einstellungen

Klicken Sie auf **Einwahl ins Internet** und kontrollieren Sie, ob die ISP-Einstellungen korrekt sind.



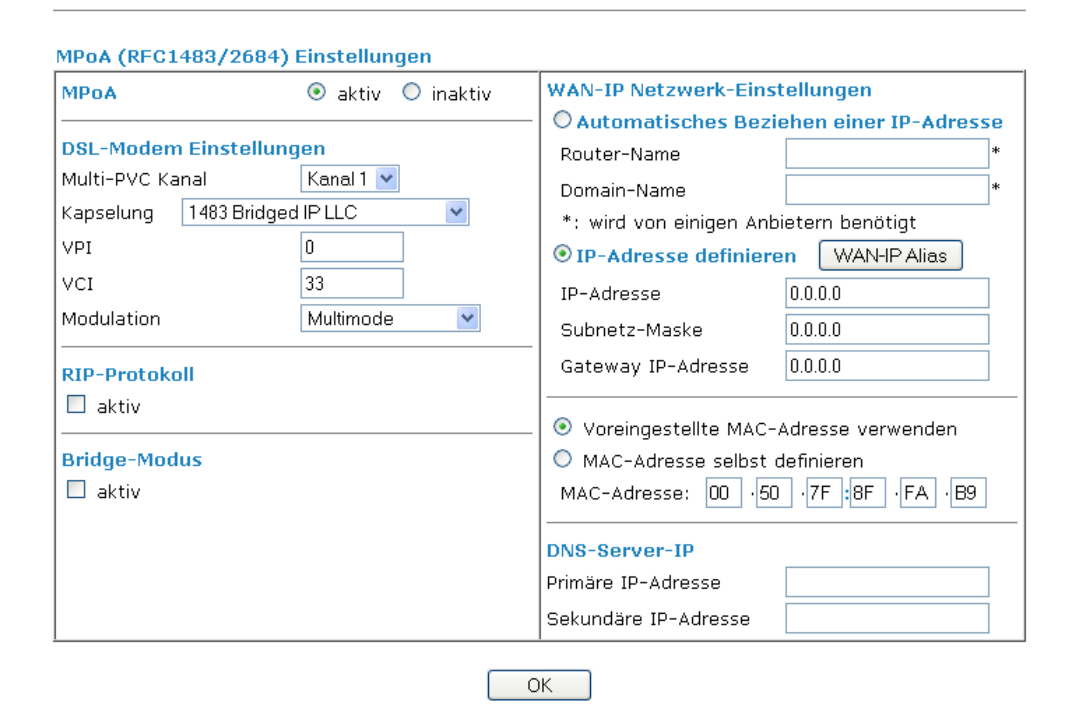
Für PPPoE/PPPoA-Benutzer

1. Prüfen Sie, ob **Aktiv** gewählt ist.
2. Prüfen Sie, ob der **Benutzername** und das **Passwort** den von Ihrem **ISP** erhaltenen Werten entsprechen.



Für MPoA-Benutzer

1. Prüfen Sie, ob **Aktiv** gewählt ist.
2. Prüfen Sie, ob alle Parameter der **DSL-Modem Einstellungen** mit den korrekten Werten von Ihrem ISP eingegeben wurden. Überprüfen Sie insbesondere, ob die Kapselung richtig gewählt wurde (sollte der Einstellung im **Schnellstart-Assistent**en entsprechen).
3. Prüfen Sie, ob **IP-Adresse, Subnetz-Maske** und **Gateway** richtig eingestellt sind (gemäß den Werten von Ihrem ISP), wenn Sie **IP-Adresse definieren**.



6.5 Auf Werkseinstellungen zurücksetzen (Factory-Reset)

In vielen Fällen kann eine fehlerhafte Konfiguration durch Wiederherstellung der Standardeinstellungen korrigiert werden. Versuchen Sie, den Router per Software oder Hardware zurückzusetzen.



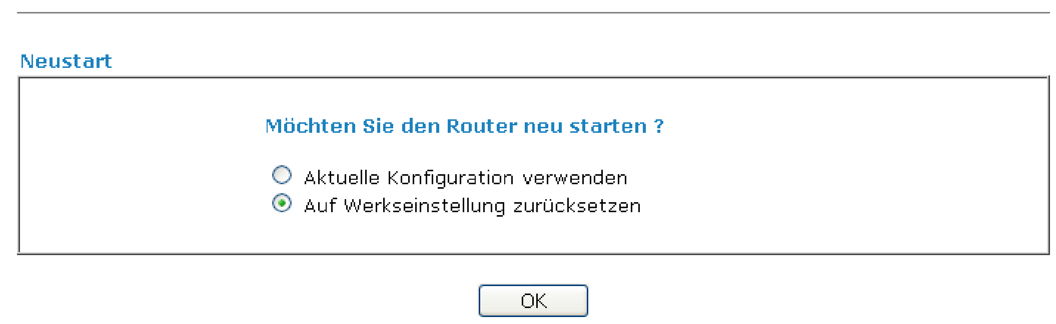
Warnung: Die Betätigung der Taste **Werkseinstellung** führt zum Verlust aller nachträglichen Einstellungen. Sorgen Sie dafür, dass Sie alle nützlichen Einstellungen notiert haben, bevor Sie diese Taste drücken. Per Werkseinstellung ist das Passwort leer.

Software-Reset

Sie können den Router über die Web-Seite auf die Werkseinstellungen zurücksetzen.

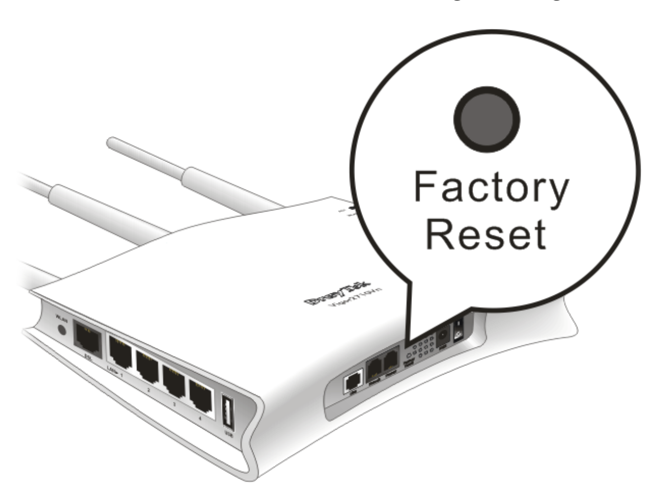
Gehen Sie zum **Systemmanagement** und wählen auf der Seite **Neustart**. Der folgende Dialog erscheint. Wählen Sie **Auf Werkseinstellung zurücksetzen** und klicken Sie auf **OK**. Nach ein paar Sekunden setzt der Router alle Einstellungen auf die Werkseinstellungen zurück.

Systemmanagement >> Neustart



Hardware-Reset

Während Router in Betrieb ist (blinkende ACT LED), drücken Sie auf den **Factory Reset** Knopf und halten Sie ihn mindestens fünf Sekunden lang gedrückt. Sobald die **ACT LED** schnell zu blinken beginnt, lassen Sie den Knopf los. Der Router wird daraufhin mit den Standardeinstellungen neu gestartet werden.



Nach Wiederherstellung der Werkseinstellungen können Sie die Router-Einstellungen erneut Ihren persönlichen Anforderungen entsprechend konfigurieren.

6.6 Technische Hilfe

Falls der Router trotz vieler Bemühungen immer noch nicht ordnungsgemäß funktioniert, nehmen Sie bitte umgehend zu Ihrem Fachhändler Kontakt auf.

Falls Sie irgendwelche Fragen haben, wenden Sie sich bitte per E-Mail an support@draytek.de.